Legislative Council Panel on Transport
Subcommittee on Matters Relating to Railways

Incident of the new signalling system testing on Tsuen Wan Line on 18 March 2019

(Information Paper)

Preface

Railway safety is of utmost importance. Both the Government and the MTR Corporation Limited (MTRCL) are very concerned about the incident on 18 March 2019 where two trains collided near Central Station during non-traffic hours drills of the new signalling system.

2. After the incident, the MTRCL immediately set up an Investigation Panel, consisted of local and overseas experts and senior MTR personnel, to conduct in-depth investigation on the incident from various angles. The Investigation Panel has completed the investigation and submitted a report to the Electrical and Mechanical Services Department (EMSD) on 17 June 2019. The EMSD has also completed its independent investigation and submitted a report to the Transport and Housing Bureau on 5 July 2019.

3. The paper reports on the respective investigation results and follow-up measures recommended by the MTRCL's Investigation Panel and the EMSD.

Signalling System Replacement Project

4. In January 2015, the MTRCL awarded a contract to Alstom-Thales DUAT Joint Venture (ATDJV)[1] for the upgrading of the signalling systems of seven railway lines (Tsuen Wan Line, Island Line, Kwun Tong Line, Tseung Kwan O Line, Disneyland Resort Line, Tung Chung Line

[1] The contractor of the new signalling system is a joint venture between Alstom Hong Kong Limited (Alstom) and Thales Transport & Security (Hong Kong) Limited (Thales). Both headquarters are located in France. "Communications Based Train Control" technology will be provided by the technology department of Thales in Canada. The MTRCL awarded the contract of $3.3 billion to this contractor in January 2015.

and Airport Express) after a competitive tendering process. The signalling system is essential to the safe operations of train services in the railway network. Railway lines are divided into blocks and only one train is allowed in each of these blocks at any one time in order to ensure trains are kept at a safe distance. The present signalling system of the above-mentioned seven existing railway lines adopts a fixed block concept[2]; while the new system, capitalised on a "Communications Based Train Control" ("CBTC") technology[3], will adopt a moving block concept with a view to increasing train frequency and capacity while maintaining a safe distance between trains.

5. The contract between the MTRCL and the signalling system contractor has specified the provision, performance and functions of the Primary, Hot-standby, and Warm-standby Computer Systems. Signalling systems are generally operated on the Primary and Hot-standby Computer Systems[4]. With a view to further enhancing the availability and expediting the recovery time of the new signalling system, the MTRCL has also specified in the contract that a Warm-standby Computer System[5] should be provided. The Primary, Hot-standby and Warm-standby Computer Systems are identical in terms of hardware and are loaded with the same software. They are configured to perform respective functions through a hardware identity plug.

6. As stated in the system specifications of the contract, it is the clear and unambiguous responsibility of the contractor to design the signalling system, develop the proprietary hardware and software, and carry out simulation and on-site tests, confirm and verify the safety and reliability of the system for operations. The relevant system development

---

[2] Under the fixed block concept, when there is a train in a certain fixed block, the signalling system will command the following train not to enter into that block.

[3] The new signalling system uses wireless communication to transmit trains information such as location and speed to the control computer. The computer then calculates the safety distance required between trains.

[4] Hot-standby Computer System is in hot-standby mode. It is fully sychronised with the Primary Computer System at all times. If the Primary Computer System is not running smoothly, it will automatically be switched to the Hot-standby Computer System.

[5] Warm-standby Computer System is in warm-standby mode. When the active primary computer system is in operation, the tertiary computer system remains in the warm-standby mode and obtains partial data from the Primary Computer System. Therefore, the data of the active Primary Computer System and the Warm-standby Computer System are not synchronised. When the Primary and Hot-standby Computer systems do not run smoothly, it will automatically be switched over to the Warm-standby Computer System to control the overall train operations.

and assessment are both responsibility of the contractor. As the end-user of the system and the railway service provider, the MTRCL would examine the tests conducted by the contractor on the new system and formulate various scenarios derived from past operating experience for on-site testing.

7. The MTRCL has all along adopted a stringent approach at each and every stage of the signalling replacement project, including the determination of specification, tendering, design, installation, simulation testing, on-site system testing, as well as scenario testing in order to ensure the safety and reliability of the new signalling system before it is put into service. To further ensure the safety of the new signalling system before it is put into passenger service, the MTRCL has also appointed an Independent Safety Assessor ("ISA") to assess the system safety assurance processes adopted by the contractor, and to provide a safety endorsement document upon satisfactory completion of the assessment. ISA was involved in the new signalling system replacement project according to its terms of reference with focus on the safety assessment before the commencement of passenger service which, however, does not include the assessment of drills.

8. The testing of new signalling system was conducted prudently and incrementally by phases. Since late 2016, on-site tests of the new signalling system have been carried out in non-traffic hours at different sections on Tsuen Wan Line, and full-line testing during non-traffic hours commenced in early 2018. The whole signalling system replacement project and the on-going tests are implemented in accordance with industry standards.

Details of the Incident

9. On 18 March 2019, the drill was being conducted with the new signalling system on Tsuen Wan Line at non-traffic hours to enable the Operations Project Team to familiarise themselves with the system operations. The Operations Project Team also had a drill on the contingency measures and recovery procedures for situations where the Primary and Hot-standby Computer Systems became unable to function normally and were automatically switched to the Warm-standby Computer System to see whether the Warm-standby Computer System could continue to operate smoothly.

10. During the drill at around 2:44 am, the first train car of an MTR train, while entering the platform of Central Station through a crossover, collided with another train that was departing Central Station for Admiralty Station through the same crossover at the same time. The collision damaged the second to fourth cars of the latter train. Please refer to **Annex 1**.

11. Affected by the incident, train service between Central and Admiralty stations on Tsuen Wan Line was suspended on 18 and 19 March, while service between Admiralty and Tsuen Wan stations was maintained at an interval of 3.5 minutes during peak hours. Tsuen Wan Line service resumed normal on 20 March. The chronology of events is at **Annex 2**.

12. As a matter of prudence, the MTRCL suspended all train tests of the new signalling system immediately and conducted in-depth investigation of the incident.

MTRCL Investigation Panel's Findings

13. According to the system specifications provided to the contractor by the MTRCL, the contractor shall provide a Warm-standby Computer System in addition to the Primary and Hot-standby Computer Systems to enhance the availability of the system and allow swift response during incidents.

14. As a contractual requirement, the design of the Warm-standby Computer System software should avoid common mode failure. In other words, the contractor should strive to avoid the possibility of transferring data causing system failures from the Primary and Hot-standby Computer Systems to the Warm-standby Computer System. Hence the system designed by the contractor should only transfer some data from the Primary and Hot-standby Computer Systems to the Warm-standby Computer System. And before taking over the function of the Primary and Hot-standby Computer Systems to control the train operations, the Warm-standby Computer System should re-create those data which are not transmitted, including "Conflict Zone Data" which are essential to prevent two trains from running on conflict routes at the same time. In June 2017, the contractor discovered the software was not coded as originally intended as stated above, thus initiated a software change in July 2017.

15. Crossovers are necessary and unavoidable in a railway system to facilitate incident handling and deploying trains between different railway lines. Under any circumstances, only one train should be allowed in each of such crossover. "Conflict Zone Data" above refers to such data related to the crossovers.

16. The designs of the Primary, Hot-standby and Warm-standby Computer Systems are at **Annex 3**.

17. Investigation of the Investigation Panel revealed that the contractor's software design and development team had committed three software implementation errors during the software change in July 2017, resulting in programming errors in the software which caused the train collision incident on 18 March -

(a) the contractor has not clearly specified in their internal software development documents for the software change, that the transmission of data should exclude the transfer of "Conflict Zone Data". As a result, the contractor did not derive specific testing whether conflict zone protection existed in its subsequent simulations, on-site testings, risk assessment and safety analysis.

(b) irrespective of the first implementation error, the contractor had excluded the transfer of the "Conflict Zone Data" from the Primary and Hot-standby Computer Systems to the Warm-standby Computer System during the software change. Nonetheless, its software design and development team had made a software implementation error which caused the Warm-standby Computer System failing to re-create the "Conflict Zone Data" properly. The details of the software implementation error are at **Annex 4**; and

(c) the software logic so built by the contractor did not stop the Warm-standby Computer System from taking over as the Primary Computer System and control the train operations even in the absence of "Conflict Zone Data", i.e. the Warm-standby Computer System controls the train operations when there is no information related to the crossovers, resulting in the scenario where the two trains were allowed to enter the crossover at the same time and collided.

18. The Investigation Panel considered that the above three software implementation errors reflected the contractor's inadequacies in the areas of software quality assurance, risk assessment and simulation tests in relation to this software change.

19. The hardware and software of the new signalling system under testing are different from that of the existing signalling system. They are two separate systems. At the time of the incident, scenario testings of the new signalling system were being conducted on Tsuen Wan Line and the existing signalling system was completely segregated. All signalling trackside and trainborne equipment were controlled by the new system at the material time. Hence, the Investigation Panel opined that the incident was not related to the existing signalling system, and incidents of similar nature would not occur to the existing operations.

EMSD's Investigation Findings

20. The EMSD conducted an independent, in-depth and comprehensive investigation into the cause of this incident, and sought assistance from an overseas railway safety consultant, Professor Roderick Smith of the Imperial College and Professor Felix Schmid of the University of Birmingham, to provide expert advice. The EMSD has completed its independent investigation on 5 July and submitted the investigation report to the Transport and Housing Bureau on the same day. The report has also been uploaded to the website of EMSD for public access. In carrying out the investigation, the EMSD has:

(a) reviewed over 250 documents and records, including traffic notices of the control center, safety briefing records, briefing records for drills and exercises, train logs, trainborne signalling logs of the incident trains and zone controller alarm logs on the day of the incident;

(b) conducted more than 65 meetings, including with the project team staff, Operations Control Center staff who were involved in the testing on the day of the incident, station staff and train captains of the MTRCL, and project team staff of the ATDJV;

(c) reviewed the software programming versions of the incident zone controllers and train-borne signalling equipment as well as conducted simulation tests on the three incident zone controllers.

21. The EMSD had thoroughly reviewed the MTRCL's Investigation Panel Report submitted on 17 June 2019 and accepted the investigation outcome of the Investigation Panel on the cause of the incident, which was the programming error in the software of the new signalling system as a result of multiple implementation errors of the contractor. This finding aligns with the finding of the EMSD's independent investigation. The investigation of the EMSD also identified the following causes of the incident:

(a) as the design requirements of the software of the concerned system was poorly specified by the system contractor, coupled with an inadequate verification and validation process of the software, the programming error was introduced in July 2017 during software rectification of the new signalling system by the system contractor. Moreover, such error was not identified by the system contractor in the verification and validation process during various system testing / software upgrades;

(b) the potential risk arising from the introduction of the Warm-standby Computer System was not comprehensively included in the risk assessment of the system contractor; and

(c) the provision of Warm-standby Computer System is a unique and non-standard design of the contractor, which is different from its standard signalling system products. However, simulation tests to the maximum extent possible were not conducted by the contractor prior to the site tests (in particular regarding the switch-over among the Primary, Hot-standby and Warm-standby Computer systems and the function relating to the automatic train protection system).

22. Moreover, the EMSD considered that the MTRCL's Investigation Panel Report mainly focused on the deficiencies of the contractor in software development and system implementation processes. The Report did not mention the roles of the MTRCL Operations Project Team in overseeing the project implementation. In any case, the EMSD considered that, having regard to the significance of this project and the fact that the system design being a non-standard one, the MTRCL should avoid over-reliance on the contractor but ought to be extra vigilant at all times.

MTRCL's Follow-up

23. The MTRCL's Investigation Panel has made a number of recommendations to the contractor and the MTRCL in the Report. The contractor is in the process of implementing the following improvement measures -

(a) replaced the software design and development team responsible for the software issue after the incident. The contractor will fix the software change issue and will confirm with substantiation that the software development quality would not be further impacted;

(b) will enhance the software coding and testing practices, including the appointment of additional external Independent Software Assessor (ISWA) to strengthen the software development process and prevent the recurrence of similar incidents; and

(c) will review, re-check and demonstrate that its software development approach adheres to international standard and fail-safe principle, and conduct risk assessment in its software implementation with support from the Investigation Panel's experts.

24. The Investigation Panel appreciated that the contractor has the responsibility to ensure the safety of the new signalling system, including the provision of a safe and reliable signalling system for testing. The Investigation Panel also suggested the MTRCL to be more vigilant and strengthen its monitoring of the contractor in implementing the recommendations so as to rebuild public confidence. Accordingly, the MTRCL will take the following measures:

(a) expand the existing scope of ISA from assuring the safety before the system being put into passenger service to cover the safety assurance relating to on-site train testing;

(b) upgrade the MTRCL Training Simulator in Hong Kong currently set up for training purposes to perform more scenario simulation tests[6] where practicable; and

[6] Currently, simulation tests can only be conducted at the contractor's laboratories overseas.

(c) establish a joint safety Test and Commissioning Panel with the contractor (together with inputs from ISA as noted in (a) above) to manage the on-site testing and explore together with the Investigation Panel's experts different options, including the merits of developing the Warm-backup Computer System by phases.

EMSD's follow-up

25. The EMSD notes the MTRCL's Investigation Panel has made a number of recommendations to the contractor and the MTRCL (i.e. paragraphs 26-27 above) and agrees that such recommendations aim to rectify the programming error and enhance the development and testing process of the new signalling system, with a view to preventing recurrence of similar incident. The EMSD will closely monitor the MTRCL's full implementation of the improvement measures and assess their effectiveness. The Government will only allow the MTRCL to resume dynamic train testing of the Tsuen Wan Line new signalling system after the MTRCL has fully completed the remedial work and the EMSD has confirmed the safety of the new signalling system upon inspection.

Conclusion

26. The Government and MTRCL attach great importance to this incident. The MTRCL will actively implement the improvement measures as recommended by the Investigation Panel. The MTRCL will resume train tests of the new signaling system only after safety is assured and the Government's consent is obtained.

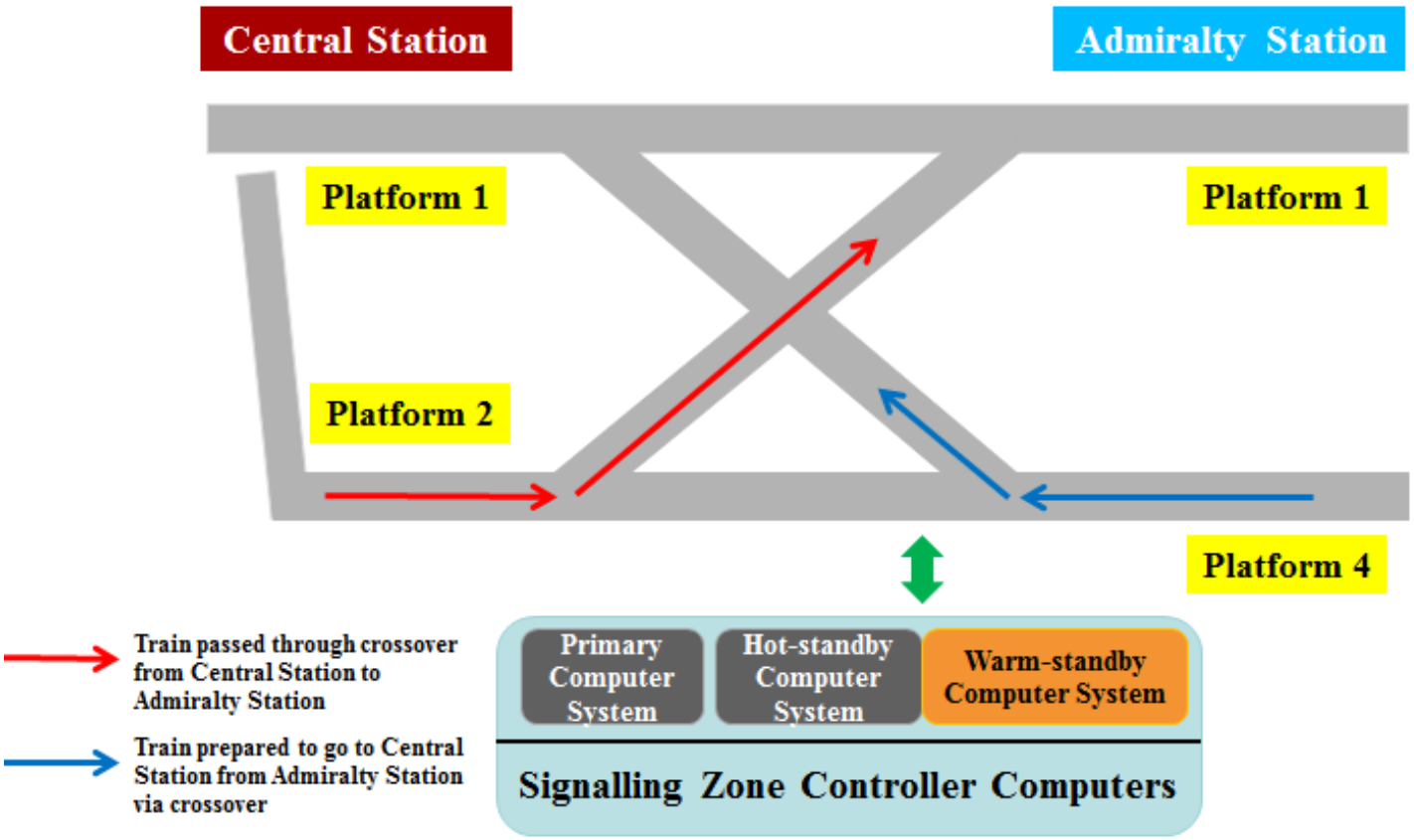
27. Members are invited to note this paper, the investigation report of the MTRCL Investigation Panel at **Annex 5**, and the EMSD's investigation report at **Annex 6**.

Transport and Housing Bureau
Electrical and Mechanical Services Department
MTR Corporation
July 2019

Annex 1

Incident of the new signalling system testing on Tsuen Wan Line on 18 March 2019

Diagram of the incident



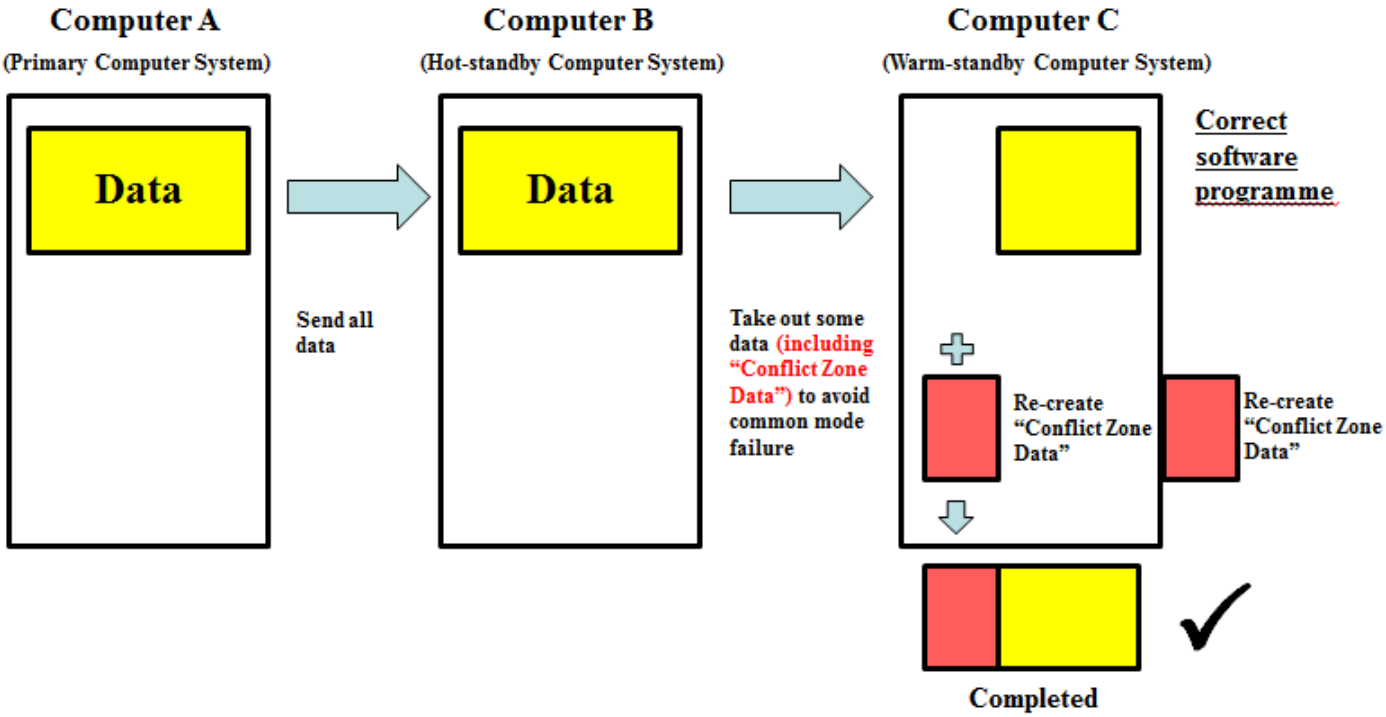
Annex 2

Incident of the new signalling system testing on Tsuen Wan Line on 18 March 2019

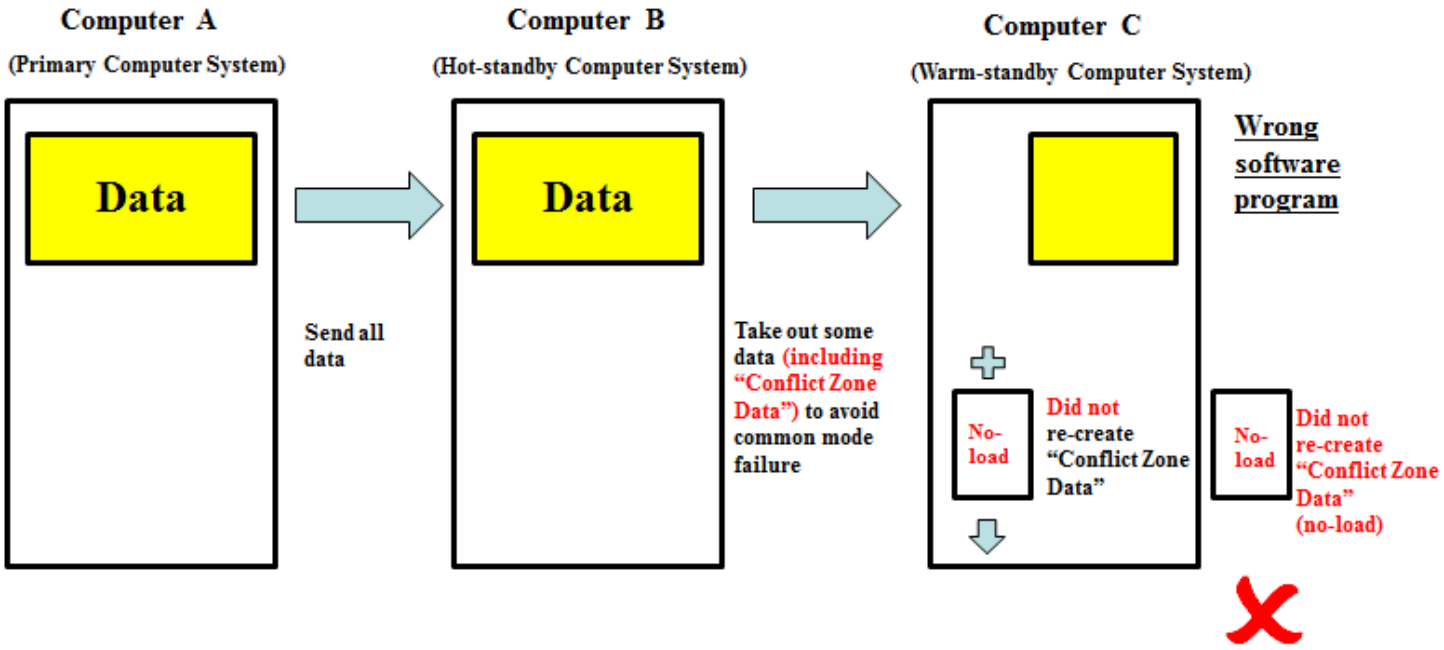
Time	Issue
18 March 2019	
2:44 a.m.	Two trains collided nearer Central Station.
2:54 a.m.	Fire Services Department and Hong Kong Police Force were informed. The two drivers were sent to hospital for medical treatment or inspection, and were discharged in the morning of the same day.
2:56 a.m.	Transport Department (TD) was informed of the incident.
3:03 a.m.	Electrical and Mechanical Services Department (EMSD) was informed.
3:17 a.m.	TD was informed regarding the service disruption on Tsuen Wan Line on the day.
4:00 a.m.	"Red alert" issued by the MTRCL. Passengers were informed of the Tsuen Wan Line service disruption through Traffic News and media. Train service between Admiralty Station and Central Station of Tsuen Wan Line was temporarily suspended.
6:30 a.m.	Media briefing on the latest development and train service update.
11:30 a.m.	Media briefing on the latest development including the announcement of setting up an investigation panel to look into the cause of the incident.
2:00 p.m.	The MTRCL met the signalling system contractor and requested the latter to submit a report and facilitate the investigation.
5:00 p.m.	Media briefing on the initial observations after meeting with the contractor.
19 March 2019	
Whole Day	Recovery works in progress.
6:30 a.m.	Media briefing on the recovery works progress and continued suspension of train service between Admiralty Station and Central Station for Tsuen Wan

	Line.
6:00 p.m.	Media briefing on the follow-up action of the Board of the MTRCL and explanation of the incident.
11:00 p.m.	Two bogies of one of the trains were re-railed.
20 March 2019	
0:00 a.m. to 1:15 a.m.	Recovery works in progress.
1:15 a.m.	The trains were moved to the sidings at Admiralty Station and safety inspection was conducted after recovery works completed.
Time	**Issue**
4:45 a.m.	Passengers was informed that the trains were moved away from the main line, recovery works were completed and the Tsuen Wan Line train service would resume on the day through Traffic News and media.
10:00 a.m.	Media briefing on the train operations after service resumption, and the processes and challenges of recovery works.

Annex 3


Computer A
(Primary Computer System)
Data
Send all data
Computer B
(Hot-standby Computer System)
Data
Take out some data (including "Conflict Zone Data") to avoid common mode failure
Computer C
(Warm-standby Computer System)
Correct software programme
Re-create "Conflict Zone Data"
Re-create "Conflict Zone Data"
Completed

Annex 4


Computer A
(Primary Computer System)
Data
Send all data
Computer B
(Hot-standby Computer System)
Data
Take out some data (including "Conflict Zone Data") to avoid common mode failure
Computer C
(Warm-standby Computer System)
Wrong software program
No-load
Did not re-create "Conflict Zone Data"
No-load
Did not re-create "Conflict Zone Data" (no-load)

Confidential

Investigation Panel Report on Train Collision Incident at Central Station (Tsuen Wan Line) during Non-traffic Hours on 18 March 2019

Submitted by:

Adi Lau	Peter Ewen
Operations Director	**Engineering Director**

Investigation Panel Co-Chairpersons

Date: 17 June 2019

Table of Contents

Executive Summary

1. Introduction

2. The Investigation Panel

3. Background

   3.1 Signalling Replacement Project

   3.2 Testing and Simulation

   3.3 Safety Assurance

4. The Incident

5. Causes of the Incident

6. Findings

7. Conclusions

8. Recommendations

Annex 1 Overall Programme of Simulations and Testing

Annex 2 Illustration of the Scenario

Annex 3 Data Transfer among the Three Computers A, B and C

Executive Summary

During the non-traffic hours on 18 March 2019, a drill was conducted on the new signalling system provided by the contractor Alstom-Thales DUAT Joint Venture (ATDJV) on the Tsuen Wan Line (TWL). The objective of the drill was to familiarize the operators with the system behaviour and the application of operational procedures in a situation in which both the Primary and Hot-standby computers failed and there was a need to switch to the Warm-standby computer.

At around 02:44 hours, a non-passenger train which was heading to a platform of Central Station (CEN) through a crossover collided with another non-passenger train that was departing from CEN for Admiralty Station (ADM) through the same crossover, causing damage to both trains. Both Train Captains were sent to hospital for medical checks, and they were discharged on the same day.

The Corporation was greatly concerned about the incident and therefore set up an Investigation Panel with membership consisting of MTR senior personnel and external experts to investigate and identify the cause of the incident, and make recommendations to prevent the recurrence of similar incident.

The investigation concluded that ATDJV had created a software issue which led to the missing of conflict zone protection at the crossover, resulting in the aforementioned two trains being allowed to enter into and collide at the crossover. The software issue was created as a result of software implementation errors made during the process of performing a software change.

The Panel further concluded that the software implementation errors reflected inadequacies in ATDJV's software development process with respect to software quality assurance, risk assessment and the extent of simulation on this software change.

Recommendations were made by the Panel to ATDJV to:

(a) replace the software design and development team causing the software issue;

(b) fix the software change issue and confirm with substantiation that there are no wider implications in software development quality;

(c) enhance the software coding and testing practices to avoid future programming errors and introduce effective and traceable measures for detection of any programming errors; and

(d) develop a full range of effective measures, including but not limited to (i) employing an external Independent Software Assessor to enhance the software development process for Computers A/B and C from its core product; (ii) reviewing, re-checking and demonstrating robustness on its approach with traceable evidence in applying a fail-safe principle; and (iii) conducting risk assessment in its software implementation with support from the Panel's experts.

To assist ATDJV to address the above, the Panel recommended the MTR Operations Project Team to exercise extra vigilance and strengthen the monitoring on ATDJV's deliveries to rebuild public confidence as below:

(a) expand the scope of the Independent Safety Assessor (ISA) from safety assurance for passenger service to the inclusion of on-site train-related testing certification;

(b) upgrade the Training Simulator in Hong Kong to act as a testing simulation tool to perform more scenario simulation tests as far as practicable;

(c) establish a joint safety Test & Commissioning Panel

(MTR/ATDJV together with input from the ISA) to manage on-site testing; and

(d) explore together with the Panel's experts on the merits, if any, for staging the development of the Warm-standby computer, or any other technically appropriate alternatives proposed by ATDJV.

Only with consent obtained from the Government, will train testing of the new signaling system during non-traffic hours be allowed to resume.

1. Introduction

1.1 At around 02:44 hours of 18 March 2019, which was during non-traffic hours, a drill was conducted on the new signalling system on the Tsuen Wan Line (TWL). A non-passenger train which was heading to a platform of Central Station (CEN) through a crossover, collided with another non-passenger train that was departing from CEN for Admiralty Station (ADM) through the crossover at the same time, causing damage to both trains.

2. The Investigation Panel

2.1 The Corporation was greatly concerned about the incident and therefore set up an Investigation Panel to investigate and identify the cause of the incident, and make recommendations to prevent the recurrence of similar incident.

2.2 The Panel was chaired jointly by Adi Lau, Operations Director and Peter Ewen, Engineering Director. Membership consisted of senior MTR personnel in the fields of Operations and Engineering as well as external experts, namely Gab Parris, Peter Sheppard and Joseph Wong of a globally recognized engineering consulting firm WSP, and Prof. S.L. Ho, the Associate Vice President (Academic Support), The Hong Kong Polytechnic University.

3. Background

3.1 Signalling Replacement Project

3.1.1 Signalling systems are essential for safe operation of train services in railway networks. To increase train frequency and capacity as well as to progressively replace the existing assets, in January 2015 MTR awarded a competitively tendered contract for the replacement of the signalling systems on seven railway lines (Tsuen Wan Line, Island Line, Kwun Tong Line, Tseung Kwan O Line, Disneyland Resort Line, Tung Chung Line and Airport Express). The contract was awarded to Alstom-Thales DUAT Joint Venture (ATDJV), a joint venture between Alstom Hong Kong Limited (Alstom) and Thales Transport & Security (Hong Kong) (Thales). Both Alstom and Thales are internationally renowned railway infrastructure suppliers having proprietary rights and knowledge over their products and technology.

3.1.2 The TWL signalling system is divided into two control zones. In each control zone, the new signalling system comprises three signalling zone controller computers as required by the contract, namely Computer A as the Primary Computer, Computer B as the Hot-standby computer and Computer C as the Warm-standby computer. Computers A, B and C are of the same hardware and loaded with common software. They are configured to perform functions of Computers A, B and C through a hardware identity plug which allows the common software to process dynamic data among the three computers correspondingly. Computer C only receives selected dynamic data from Computers A/B so as to avoid common mode failure. This configuration aims to improve system availability and service recovery through higher resilience. The Warm-standby arrangement is novel in ATDJV's signalling system application. Furthermore, Computer C is housed at a different station which enhances system security through access control and diverse power supply.

3.2 Testing and Simulation

3.2.1 The MTR Operations Project Team managed the replacement work by applying a method widely adopted in the railway signalling industry. This method, which was implemented by the contractor, included software simulation testing in its laboratory and on-site testing to ensure the new signalling system was developed and matured in a safe and controlled manner. All related testing activities were conducted in a step-by-step and incremental approach along key stages with certification protocols and safety documentation issued by ATDJV. The diagram at Annex 1 shows the overall programme of the simulations and testing.

3.2.2 ATDJV started on-site train testing during non-traffic hours on TWL in December 2016 and the scope of test was progressively extended from one train to multiple trains.

3.2.3 Through stage-by-stage system maturity testing, incremental confidence was built up on the readiness of the new signalling system to start drills on the system operation and operator familiarization of the system behaviour in February 2019. The drills were jointly performed by the MTR Operations Project Team and ATDJV.

3.2.4 Based on the previous simulations, which had been conducted with the common software installed on all computers while not repeating in Computer C for the completed simulations done on the common software, and also testing of its specific transition function from Computer A/B to C, ATDJV issued related safety documentations giving the MTR Operations Project Team the confidence in allowing Computer C to become the Primary Computer for the drill. The objective of the drill was to familiarize the operators with the system behaviour. Through the drill, the operators would have the opportunity to become conversant with the multitude of train service situations expected in future day-to-day operations. The drill would also enable fine-tuning of the operational procedures if required before the new signalling system is eventually put into passenger service.

3.3 Safety Assurance

3.3.1 ATDJV has the responsibility to supply a safe signalling system in accordance with the contractual obligations and design requirements. The MTR Operations Project Team required ATDJV to define the scope and the extent of simulations and tests to ensure that a safe signalling system is delivered in accordance with international standards per their responsibility.

3.3.2 ATDJV had a project safety team for vetting and certifying software safety for the on-site testing and drills. Besides, they also separately deployed an independent safety team to assess and certify the system safety before the new signalling system would be certified for passenger service.

3.3.3 In addition to the ATDJV safety assurance described above and to further ensure the safety of the new signalling system before it is put into passenger service, the MTR Operations Project Team also appointed an Independent Safety Assessor (ISA) which was tasked to assess the system safety assurance processes followed by the contractor, and to provide a safety endorsement document upon satisfactory assessment of such processes. The ISA was for certification of passenger service only, but not on other earlier key project stages such as commencement of drills. Furthermore, the MTR Operations Project Team appointed an external Independent Reviewer (IR) to provide advice on project implementation risks associated with the operating railway. The ISA and IR were involved in project activities within their own scope of works as described above but neither of their mandates covered the assessment of drills.

4. The Incident

4.1 During the non-traffic hours on 18 March 2019, the MTR Operations Project Team jointly with ATDJV engineers performed the pre-planned drill to verify the handling procedures for coping with the failure of both Computer A and Computer B, thereby leading to Computer C taking over as the Primary Computer. The objective of the drill was to familiarize the operators with the system behaviour and application of

operational procedures when there are Computer failures.

4.2 At around 02:34 hours, Computers A and B were switched off sequentially to simulate the failure and Computer C took over as the Primary Computer as per the system design. All routes that had been set for trains were cancelled and all trains were stopped as expected in the switchover to the Warm-standby Computer C. The Traffic Controller (TC) in the Operations Control Centre (OCC) then had to give "Depart" commands to depart the trains one after another according to normal operational procedures to allow the resumption of train movement.

4.3 At around 02:41:32 hours, the TC gave a "Depart" command to the train berthing at CEN platform 2 in accordance with the procedure. The route for the train to go to ADM platform 1 was then set by Computer C. At around 02:43:53 hours, for normal traffic regulation, the TC disengaged the platform sequencing selection for CEN to allow the waiting train to berth at CEN platform 1 which was vacant. At around 02:44:01 hours, Computer C erroneously set conflicting routes with signal clear, causing the two trains departing within seconds in Automatic Mode to collide at the crossover outside CEN. For such an instantaneous and unexpected system behaviour, it was very challenging and difficult for the TC to respond and intervene at OCC level through the execution of command steps in calling the emergency brake of the trains in time, as the role of the TC was to manage train regulation activities and as such they would not be expected to be checking for and reacting to such unexpected system behaviour. Similarly, although the Train Captain of the train travelling to CEN platform 1 did activate the emergency brake when he saw the train travelling from CEN platform 2 to ADM platform 1, the train was not able to stop before colliding.

The diagram at Annex 2 illustrates the scenario.

4.4 Apart from one of the two Train Captains who had his right knee mildly abraded, none of the MTR staff or ATDJV staff were injured. Both Train Captains were sent to hospital for medical checks, and they were discharged on the same day.

5. Causes of the Incident

5.1 Computers A, B and C were identical in hardware and loaded with the common software but had different identity hardware plugs to configure them to initially perform as Primary, Hot-standby and Warm-standby, i.e. Computers A, B and C respectively. Before June 2017, the data transferred from Computer A to B or from Computer B to C were all identical which meant that any data corruption causing a failure in Computers A and B would be transferred into C creating a common mode failure.

5.2 To avoid common mode failure according to the contract requirement, ATDJV thus initiated a software change in July 2017. Some dynamic data was selected to be excluded (including "Conflict Zone Data" which prevents conflicting routes from being set) from the data transferal from Computer A/B to Computer C, and those excluded data should subsequently be re-created internally in Computer C. The amount of data excluded and re-created was determined by ATDJV with due consideration to the risk of common mode failure and the swift recovery time so required for Computer C to take up as the Primary Computer in case both Computer A and B fail. However, this software change initiated by ATDJV gave rise to a software issue due to a series of software implementation errors made by its software design and development team during the process of performing this software change.

5.3 Investigation revealed that ATDJV had created the software issue which was caused by the following three software implementation errors made during the process of performing this software change. First, while "Conflict Zone Data" was meant to be excluded, out of expectation it was not specified in ATDJV's internal software development document. Because of this lack of specification, no subsequent specific test, risk assessment and safety analysis, including laboratory verification simulation and on-site testing, was done by ATDJV to verify the "Conflict Zone Data" when Computer C took over as the Primary Computer. This was the first software implementation error.

5.4 Second, ATDJV excluded the transfer of the "Conflict Zone Data" from Computer A/B to Computer C, but its software design and development team made a software implementation error in failing to properly re-create the "Conflict Zone Data" internally in Computer C. This second software implementation error resulted in there being no "Conflict Zone Data" when Computer C took over as the Primary Computer.

5.5 Third, the software logic so built by the software design and development team did not stop Computer C from taking over as the Primary Computer when "Conflict Zone Data" was not available; in other words Conflict Zone protection was not available. This is considered as a software implementation error in not implementing appropriate programming logic to prevent Computer C from taking over as the Primary Computer while having no conflicting route protection.

6. Findings

6.1 The Panel found that until the incident, ATDJV was not aware of the software issue as described in Section 5 throughout its verification and validation process, including simulations done as per their process. As the said software issue was not identified by ATDJV, it was therefore not revealed to the MTR Operations Project Team either. The Panel also noted that ATDJV had issued related safety documentation giving the MTR Operations Project Team the confidence that Computer C would be safe for drills. Indeed, since 15 October 2018, there was no restriction on the number of trains used and no restriction on train separation distance required for on-site testing, in accordance with the safety documentation issued by ATDJV. Furthermore, tests had been undertaken with a procedure that allowed Computer C (as Warm-standby) to become the Primary Computer since mid-October 2018, i.e. with Computer C in full control of the system after switching over continuously. Therefore, for any on-site testing from that point, the software issue could have emerged inadvertently if Computer C had taken over as the Primary Computer, depending on the combination of many permitted and probable situational factors. The Panel

opined that the three software implementation errors made during the process of performing this software change before the incident by ATDJV were the causes of the incident.

> ***"WSP's Independent Expert Team considers that ATDJV is responsible for providing assurance to MTR that their product is safe.***
>
> ***With respect to MTR's Drills / Exercises, it is clear that those activities are purely designed to allow MTR to develop and test their operational rule book and familiarize their staff with normal and degraded mode behavior in addition to gaining confidence in the operability and reliability of the 3036 CBTC system."***
>
> ***WSP***
> ***External Expert***

6.2 The Panel also considered that the software implementation errors reflected inadequacies in ATDJV's software development process with respect to software quality assurance, risk assessment and the extent of simulation on this software change.

6.3 The Panel considered that it is the responsibility of ATDJV to formulate the extent of simulations in verifying and validating the common software installed to Computers A, B and C for performing their intended functions. ATDJV should develop the software to the required maturity through their verification and validation process. Simulations to the extent required as per their process had been done as defined in the software development document by ATDJV before the commencement of

on-site testing. Thereafter, extensive on-site testing was conducted, and iterative simulations and testing, with extra time of more than one year given, had been carried out as appropriate in building up the software maturity. Without knowing the software issue and given the results of the simulations and on-site testing conducted including switchover from Computer A/B to Computer C as witnessed by the MTR Operations Project Team, the project moved to the next stage on the basis that the software should have the maturity to allow safe execution of drills for the operators to safely familiarize themselves with the system behaviour in whatsoever operational circumstances, which was allowed as confirmed by the safety documentation provided by ATDJV. Nevertheless, the Panel opined that given the nature of the software change as revealed after the incident, a wider extent of simulation should have been formulated by ATDJV to cover possible impacts to the critical system performance even if changes were not specified clearly in the software development document.

6.4 The MTR Operations Project Team was aware that there would be a further software version to come after the drills. However, the Panel opined that there was nothing to suggest that the drills on 18 March 2019 should be withheld as the maturity of the software already in use should have been sufficient for the purpose as described in paragraph 6.3.

"It would be unreasonable for MTR to make a unilateral decision, based on no solid grounds, to suspend any drills on Build 8.3.3 and wait for the release of Build 8.3.4."

Professor S.L. Ho
External Expert

> ***"According to Thales' documentation provided (i.e. Safety Cert and SOR), it was safe to run the drill on 18th March 2019."***
>
> ***WSP***
> ***External Expert***

6.5 In the process of maturing the software, laboratory simulations had been done by ATDJV to verify the system functions were fit for on-site testing. In relation to the drills, their purpose was for the operator to have site familiarization on the system behaviour and to respond to a multitude of possible in-situ scenarios that can be experienced in real-life operations. With the understanding that the required scenario as defined by the software development document, including switching over from Computer A/B to C had been carried out before arranging the drill, the Panel opined that additional situational case scenarios could still be further included in the simulations to enhance the level of assurance.

6.6 The Panel noted that according to the original resource plan, the procedure for the drill on 18 March 2019 was planned with 4 trains. Yet, there was no longer any limitation on the number of trains according to the safety documentation issued by ATDJV at the time of the drill. In order to represent the morning peak scenario, the MTR Operations Project Team instead informed ATDJV on a number of occasions through the Commissioning Plan that they were to run 34 trains instead of 4 trains on 18 March 2019. The drill was subsequently jointly performed with 34 trains by the MTR Operations Project Team and ATDJV. Since there was no restriction in train separation distance under the procedure, and given the non-existence of conflicting route protection, the incident could have occurred with 2 trains or more as verified during the investigation. The Panel was therefore of the opinion that while the running of 34 trains resulted in raising the likelihood of revealing the unknown software issue, it was

definitely not the cause of the incident. The Panel also noted that the operators participating in the drill acted properly in accordance with the normal operational procedures for handling the scenario that would be encountered in future day-to-day operations.

6.7 The Panel has reviewed the findings and recommendations that the ISA provided previously in relation to their concerns on i) compliance with Thales' internal development processes, ii) full compliance with international standards, and iii) development process weakness and its associated risks in their core product. The Panel noted that the MTR Operations Project Team and the ISA had taken additional measures in the form of extra assessments involving a series of factory visits and extra simulation tests, with extra time of more than one year given to ATDJV, in building up the software maturity and addressing the above ISA's concerns. While noting that the ISA's findings and recommendations were for passenger service and not for drills and testing as per its remit, ATDJV did make progress in closing some findings but not yet all before the incident . The Panel has confirmed with the ISA that, based on their findings thus far, they had not identified any specific issues for cessation of the on-site tests or drills. The Panel hence concluded with due consideration on the ISA's findings and recommendations that there were no specific unsafe issues identified by, nor recommendations from, the ISA to suggest discontinuing on-site testing or drills. Nevertheless, the Panel opined that the MTR Operations Project Team should exercise extra vigilance in addressing the ISA's comments in monitoring ATDJV's deliveries in future.

6.8 The Panel opined that there was no reason to discontinue the on-site testing, including drills based upon the required safety documentation supplied by ATDJV, at the time when the incident happened. Nevertheless, the Panel opined that the MTR Operations Project Team should in future be more vigilant in assessing implications of the ISA's concerns on drills and consider expanding the ISA's scope to cover assessment of on-site testing.

"WSP Independent Expert team (in MTR's place) would have also allowed the Drills to go ahead on the basis that the required safety assurance documentation had been produced by Thales specifically for the Drills and Tests (Specific Application Safety Case with restrictions (SOR) further amended by a Safety Memo), which was underpinned by the incremental assurance and confidence gained from all previous activities and documentation produced."

WSP
External Expert

"MTR had been taking a prudent and incremental approach to gain confidence in the organization of the Tests and Drill & Exercises. Additional steps had also been taken upon receipt of the advices from the Independent Safety Assessor. Hence it was reasonable for MTR to believe the Drill on 18 March should be a routine familiarization exercise."

Professor S.L. Ho
External Expert

7. Conclusions

7.1 The Panel has reviewed the facts and factors relevant to the causes of the incident, and concluded that ATDJV had created the software issue as a result of the following three software implementation errors made during the process of performing this software change.

(a) software development document did not specify the exclusion of the "Conflict Zone Data" which led to no ensuing specific test and safety analysis to identify the unknown software issue;

(b) a software implementation error led to no re-creation of proper "Conflict Zone Data" internally in Computer C when Computer C took over as the Primary Computer; and

(c) while Conflict Zone protection was not available, subsequently Computer C still continued its process to become the Primary Computer because the software logic was so built that it did not stop Computer C from taking over as the Primary Computer, resulting in missing the conflicting route protection.

7.2 The Panel also concluded that the software implementation errors reflected inadequacies in ATDJV's software development process with respect to software quality assurance, risk assessment and the extent of simulation on this software change.

7.3 With ATDJV's weakness as set forth in paragraph 7.2, the Panel also concluded that the MTR Operations Project Team should exercise extra vigilance and additional monitoring measures on ATDJV's deliveries in future.

8. Recommendations

8.1 The Panel has made recommendations based upon on the causes and the lessons learnt from the incident.

8.2 To prevent recurrence of similar incident due to the same causes, the Panel recommended ATDJV to:

(a) replace the software design and development team causing the software issue;

(b) fix the software change issue and confirm with substantiation that there are no wider implications in software development quality;

(c) enhance the software coding and testing practices to avoid future programming errors and introduce effective and traceable measures for detection of any programming errors; and

(d) develop a full range of effective measures, including but not limited to (i) employing an external Independent Software Assessor to enhance the software development process for Computers A/B and C from its core product; (ii) reviewing, re-checking and demonstrating robustness on its approach with traceable evidence in applying a fail-safe principle; and (iii) conducting risk assessment in its software implementation with support from the Panel's experts.

8.3 To assist ATDJV to address the above, the Panel recommended the MTR Operations Project Team to exercise extra vigilance and strengthen the monitoring on ATDJV's deliveries to rebuild public confidence as below:

(a) expand the scope of ISA from safety assurance for passenger service to the inclusion of on-site train related testing certification;

(b) upgrade the Training Simulator in Hong Kong to act as a

testing simulation tool to perform more scenario simulation tests as far as practicable;

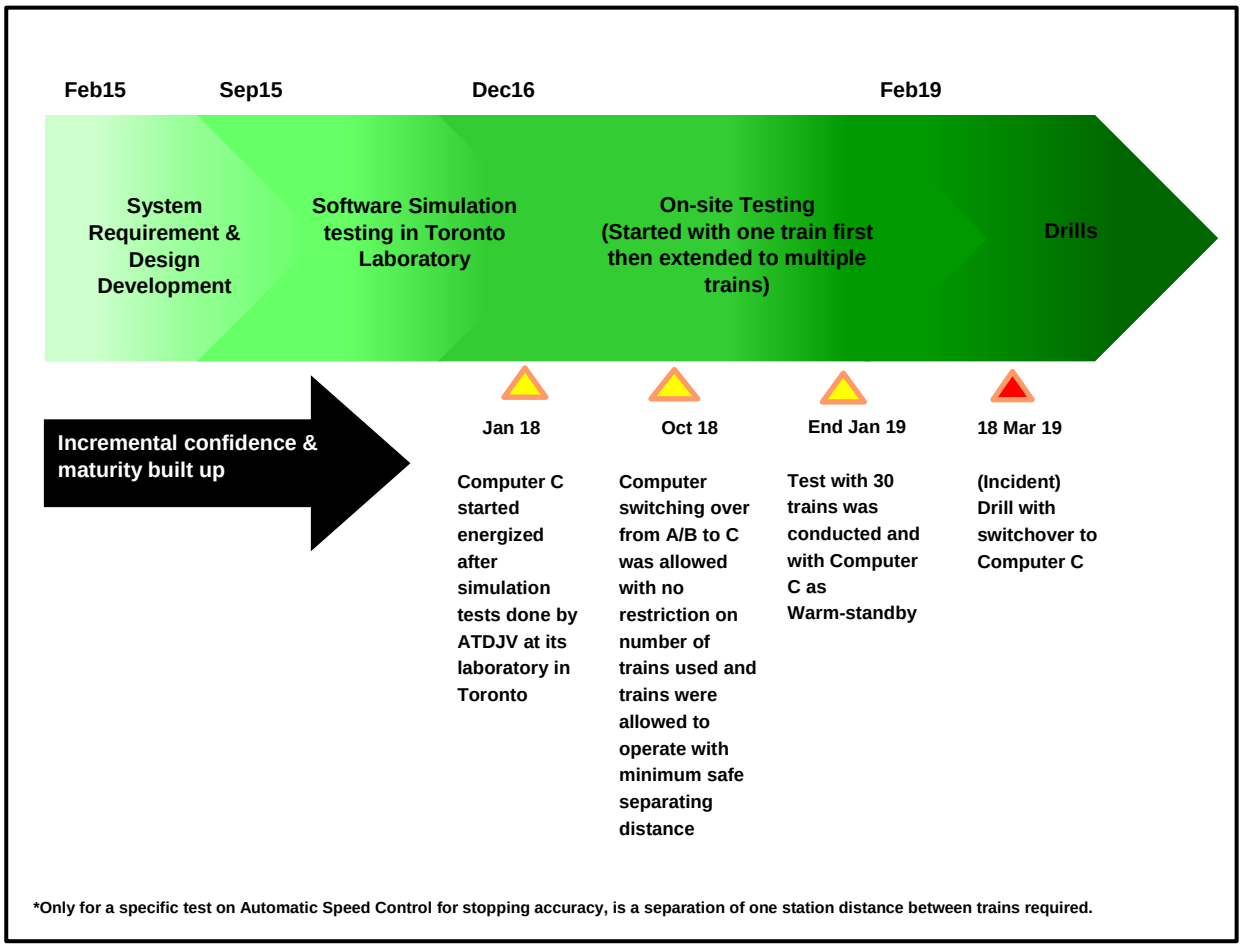
(c) establish a joint safety Test & Commissioning Panel (MTR/ATDJV together with input from the ISA) to manage the on-site testing; and

(d) explore together with the Panel's experts on the merits, if any, for staging the development of the Warm-standby Computer C, or any other technically appropriate alternatives proposed by ATDJV.

8.4 Only with the consent obtained from the Government, will train testing of the new signalling system during non-traffic hours be allowed to resume.

Annex 1

Overall Programme of Simulations and Testing



Notable activities

1. ATDJV started on-site train testing during non-traffic hours on TWL in December 2016 and the scope of test was progressively extended from one train to multiple trains.

2. In January 2018, Computer C started to be energized as Warm-standby after simulation tests done by ATDJV at its laboratory in Toronto.

3. From 15 October 2018 onwards, in accordance with the safety documentation issued by ATDJV, computer switching over from A/B to C was allowed with no restriction on the number of trains used

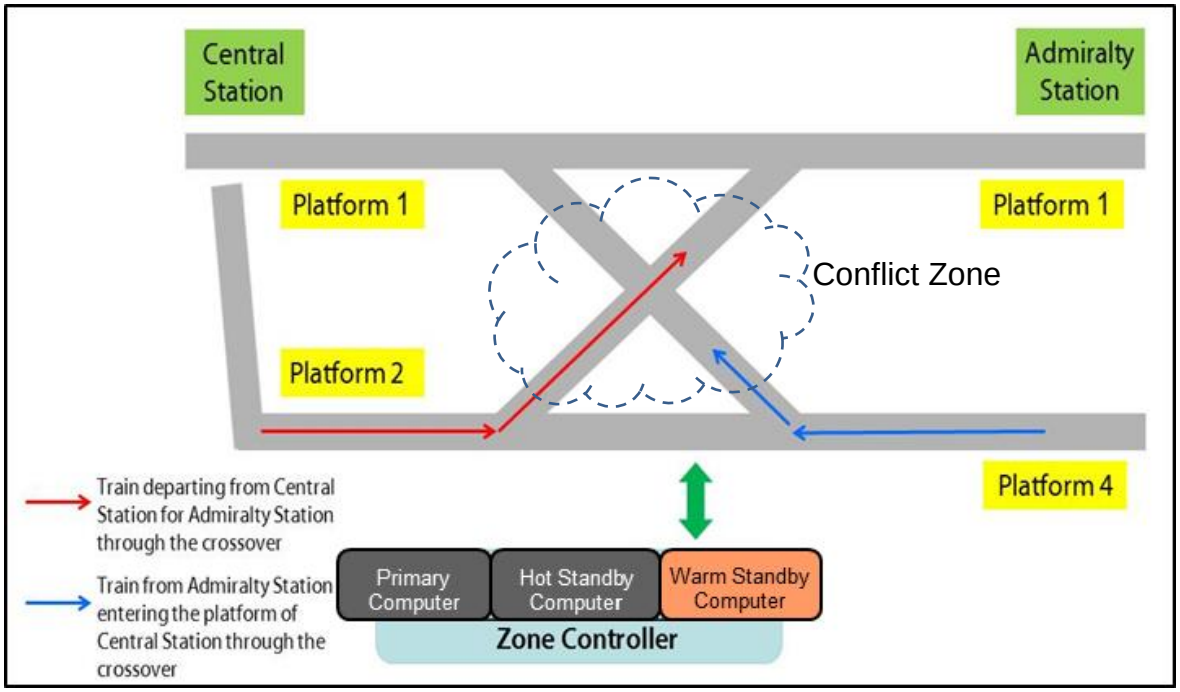
and trains were allowed to operate with minimum safe separating distance. Only for a specific test on Automatic Speed Control for stopping accuracy, was a separation of one station distance between trains required.

4. In January 2019, while there was no restriction on the number of trains, full line testing with 30 trains and with Computer C as Warm-standby was conducted. In other words, Computer C could have taken the overall operational control in case both Computers A and B had failed.

Annex 2

Incident of the New Signalling System Drill on Tsuen Wan Line on 18 March 2019

Illustration of the Scenario

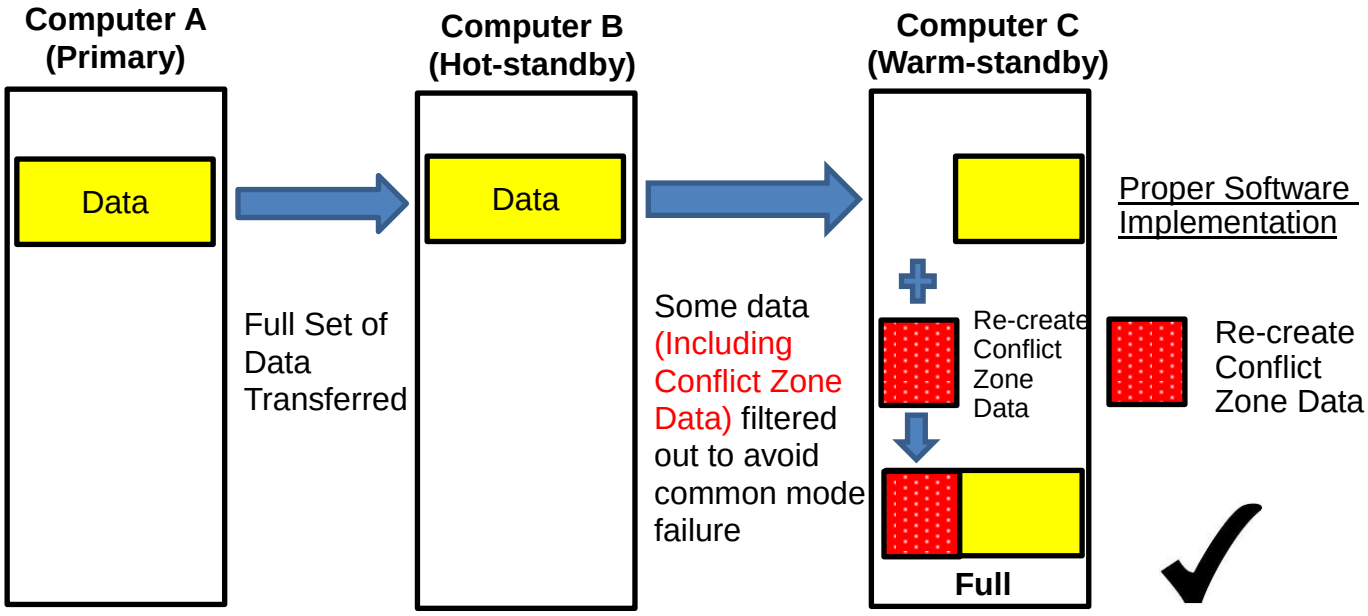


Annex 3

Data Transfer among the Three Computers A, B and C

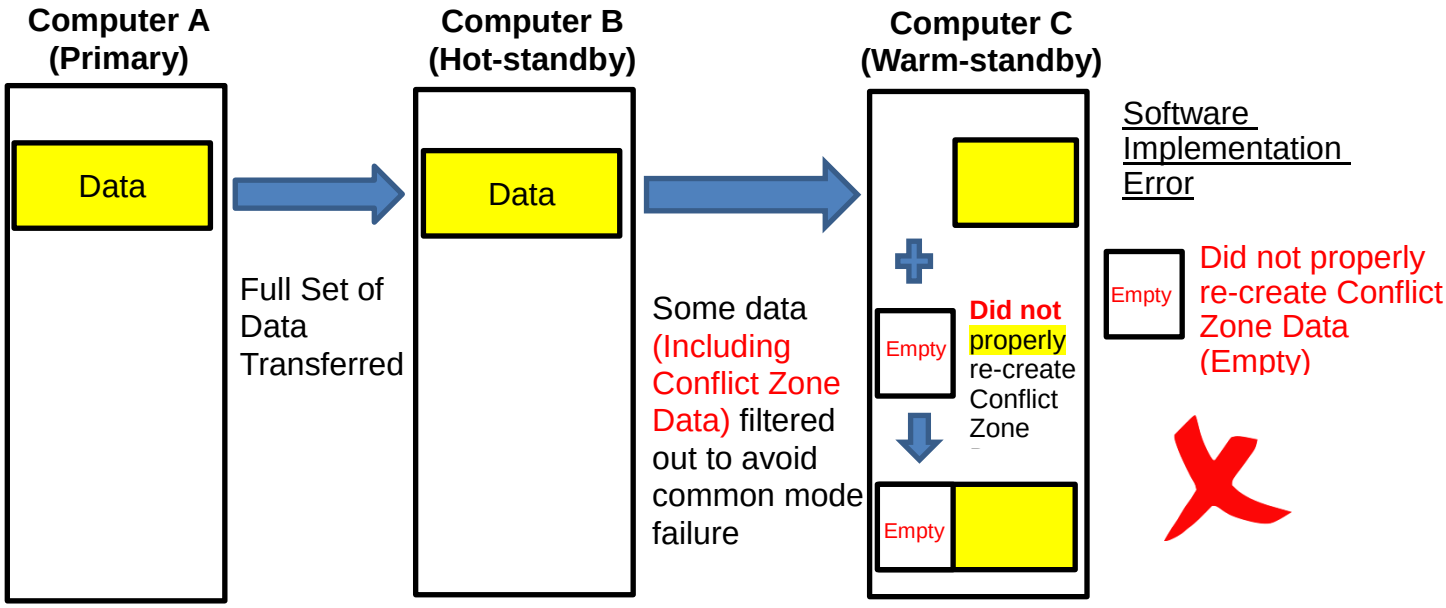
On 18 March, Computer A as "Primary" was switched off and made Computer B become "Primary", thereafter, Computer B was subsequently switched off and made Computer C become "Primary".

Design Intention developed by ATDJV



What Happened :

Software Implementation Errors resulted into an unknown software issue



Investigation Report on

Incident of the New Signalling System Testing on

MTR Tsuen Wan Line

港鐵荃灣綫

新信號系統測試事故

調查報告

Date of Incident: 18 March 2019

事故日期：2019 年 3 月 18 日

English Version

英文版

機電工程署 EMSD

Date of Issue: 5 July 2019

出版日期：2019 年 7 月 5 日

CONTENTS

	Page
Executive Summary	2
1. Objectives	4
2. Background of the Incident	4
3. Technical Information of the Incident Signalling System	7
4. Approach of Investigation	11
5. The EMSD Investigation Findings	12
6. Investigation Findings of Railway Experts Engaged by the EMSD	19
7. Conclusions	23
8. Measures Taken after the Incident	23
Appendix I – Drills and Exercises from 16 February to 18 March 2019	25
Appendix II – Sequence of Events	26
Appendix III – EMSD's views on the MTRCL Investigation Panel Report	27

Executive Summary

On 18 March 2019, a two-train collision incident happened during a drill and exercise on the new signalling system of the Tsuen Wan Line. This report presents the results of the Electrical and Mechanical Services Department's (EMSD) independent investigation into the causes of the incident.

The signalling system contractor Alstom-Thales DUAT Joint Venture (ATDJV), which is a joint venture of the Alstom Hong Kong Limited (Alstom) and the Thales Transport & Security (Hong Kong) (Thales), had been carrying out tests of the new signalling system in non-traffic hours at different sections of the Tsuen Wan Line by phases since late 2016. The tests carried out by the ATDJV for the entire section were completed in February 2019. On 16 February 2019, the MTR Corporation Limited (MTRCL) commenced the drills and exercises.

The incident occurred in non-traffic hours at 2:44 a.m. on 18 March 2019, when the MTRCL was conducting drills and exercises on the new signalling system of the Tsuen Wan Line. At the time of the incident, train T131, which was travelling from Admiralty Station to platform no. 1 of Central Station, collided with train T112, which was leaving Central Station for Admiralty Station, resulting in damage to the second to fourth cars of train T112 and derailment of two bogies of the first car of train T131. The train captains of both trains were taken to hospital for medical check and discharged on the same day.

According to our investigation findings, the cause of the incident was a programming error introduced during software rectification of the new signalling system at the design and development stage. This programming error caused a failure to re-create the data of the crossover track at Central Station after switch-over from the primary zone controller (ZC) to the warm-standby tertiary ZC. Hence, the Automatic Train Protection (ATP) system could not function as required to prevent two trains from entering the crossover track at Central Station at the same time, and led to the train collision.

The investigation also identified the following causes of the incident:

(a) the programming error, which was introduced in July 2017 during software rectification of the new signalling system, was not identified by the system contractor during various system testing / software upgrades as a result of

poorly specified design requirements and inadequate design, verification and validation processes of the software;

(b) the potential risk arising from the introduction of the warm-standby tertiary ZC was not comprehensively included in the risk assessment by the system contractor for the new signalling system; and

(c) simulation tests were not conducted to the maximum extent by the system contractor prior to the site tests, taking into account the specific requirement for a warm-standby tertiary ZC, which is a unique implementation by the supplier among the supplier's standard signalling system products.

Subsequent to the collision incident, the MTRCL had suspended all testing of the new signalling system on the Tsuen Wan Line, Island Line and Kwun Tong Line immediately. The MTRCL had also announced that all train tests for the new signalling system during non-traffic hours was suspended. The Government will allow the MTRCL to resume testing of the new signalling system of the Tsuen Wan Line only after the EMSD has ascertained the causes of the incident and remedial work has been completed satisfactorily.

The EMSD had also examined the MTRCL's Investigation Panel Report submitted on 17 June 2019 and the EMSD's views are listed at Appendix III.

Investigation Report on
Incident of the New Signalling System Testing on MTR Tsuen Wan Line
on 18 March 2019

1. Objectives

1.1 The purpose of this investigation is to identify the causes of a train collision during the new signalling system testing on the Tsuen Wan Line on 18 March 2019. This report presents the results of the EMSD independent investigation into the causes of the incident.

2. Background of the Incident

2.1 The signalling system contractor Alstom-Thales DUAT Joint Venture (ATDJV), which is a joint venture of the Alstom Hong Kong Limited (Alstom) and the Thales Transport & Security (Hong Kong) (Thales), had been carrying out tests of the new signalling system during non-traffic hours at different sections of the Tsuen Wan Line by phases since late 2016. The ATDJV commenced the full-line train tests in early 2018 and had substantially completed the tests on site, which lasted for more than two years, in February 2019. On 16 February 2019, the MTRCL commenced a series of drills and exercises (**Appendix I**) before putting the new signalling system into revenue service. From 16 February to 18 March 2019, the MTRCL conducted nine drills and exercises simulating various specific scenarios, including train fault, point failure as well as failure of both the primary and secondary zone controllers (ZC).

2.2 The incident occurred during non-traffic hours at 2:44 a.m. on 18 March 2019 (**Appendix II**), when the MTRCL was conducting the 9th drill and exercise on the new signalling system of the Tsuen Wan Line. Participating parties included the MTRCL's project staff, staff from its Operations Control Centre (OCC), station staff, train captains, and the ATDJV's engineering staff. The scenario of that particular drill and exercise was to simulate a failure of both the primary and secondary ZCs controlling the zone between Central Station and Sham Shui Po Station. The MTRCL arranged 34 trains to simulate train operation in a

situation where the warm-standby tertiary ZC[1]. would take over control from the faulty primary and secondary ZCs during peak hours, with a view to training up the MTRCL staff's response so as to maintain train operation in such situation.

2.3 According to the train logs, train T131, which was travelling from Admiralty Station to platform no. 1 of Central Station, collided with train T112 at a speed of 19 kph at the Central Station crossover track (Figure 1) at the time of the incident. At that moment, train T112 was travelling from Central Station to Admiralty Station at a speed of 31 kph when passing through the crossover track. The collision resulted in damages to the second to fourth cars of train T112 (Figure 2) and derailment of two bogies of the first car of train T131. The two train captains were taken to hospital for medical check and discharged on the same day.

Figure 1: Condition of the trains after collision

[1] Warm-standby is a redundancy system design. When the active primary ZC is in operation, the tertiary ZC remains in the warm-standby mode and obtains partial data from the primary ZC. Therefore, the data of the active primary ZC and the warm-standby tertiary ZC are not synchronised.

Figure 2: Damage to the saloon of train T112

2.4 According to the train logs and the train captains' interview records, the train captain of train T131 had pressed the emergency brake button before the collision to try to stop the train, but train T131 could not be stopped timely and collided with train T112. Moreover, according to the train logs, the ATP system could not function at that moment to restrict these two trains from entering into the crossover track at the same time. Figure 3 illustrates the train movements during the incident.

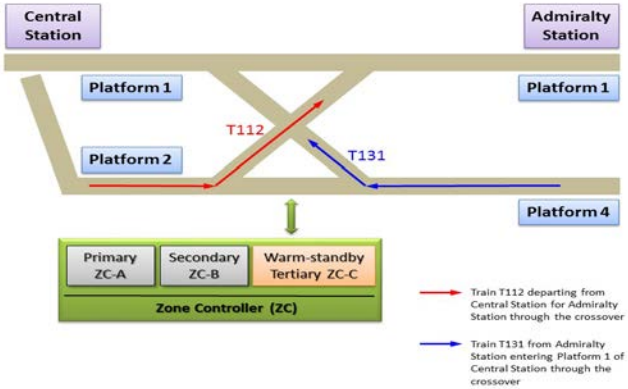


Figure 3: Train movements during the incident

2.5 The EMSD received notification of the incident at 3:03 a.m. and immediately dispatched staff to the scene for investigation.

2.6 During the drill and exercise on 18 March 2019, the existing signalling system was isolated. All trackside equipment and train-borne signalling equipment were under the control of the new signalling system. Unlike the existing signalling system and other signalling systems of the MTRCL's railway lines, this new signalling system was equipped with a unique tertiary ZC in warm-standby mode. Hence, this incident was not related to the existing signalling systems and similar incidents should not happen on existing railway lines.

3. Technical Information of the Incident Signalling System

3.1 In 2015, the MTRCL awarded a contract for upgrading the signalling systems of seven railway lines (Tsuen Wan Line, Island Line, Kwun Tong Line, Tseung Kwan O Line, Disneyland Resort Line, Tung Chung Line and Airport Express Line) to a joint venture company formed by two signalling system contractors, i.e. Alstom and Thales (known as the ATDJV). The target completion date is 2026.

3.2 A signalling system controls the safe operation of train services in railway network. Railway lines are divided into blocks and only one train is allowed in one block at any one time in order to ensure that trains are kept at a safe distance from each other. The present signalling system of the above-mentioned seven existing railway lines adopts a fixed block design[2], while the new signalling system adopts the "Communications Based Train Control" (CBTC) technology[3] using a moving block design to ensure that a safe distance between trains is still maintained even with increased train frequency and line capacity.

3.3 On 18 March 2019, the MTRCL conducted a drill and exercise on the new signalling system of the Tsuen Wan Line. Through wireless communication, trains sent information such as locations and speeds, etc. to the primary ZC, which

---

[2] With the fixed block concept, if a train is in a certain fixed block, the signalling system will send commands to the next train requesting it not to enter that block.

[3] The new signalling system uses wireless communication to transmit signals from trains (such as location and speed of trains) to the control computer. The computer then works out the safe distance required between trains.

calculated the safe distances between trains and sent limits of movement authority to the trains in order to achieve higher efficiency in train service management.

3.4 To further enhance the availability of the signalling system, the new signalling system of the Tsuen Wan Line has adopted a three-ZC configuration for train control, namely primary ZC A (ZC-A), secondary ZC B (ZC-B) and tertiary ZC C (ZC-C). This is a unique and non-standard design among its standard signalling system products of the supplier. The respective functions of the different ZCs are as follows (Figure 4):

(a) Primary ZC-A is the active ZC of the system for train control in the designated track section;

(b) Secondary ZC-B is the hot-standby ZC, which synchronises with ZC-A at all times and takes over ZC-A for train control as primary ZC when ZC-A fails;

(c) Tertiary ZC-C is the warm-standby ZC and takes over ZC-A and ZC-B as the active ZC when both ZC-A and ZC-B fail at the same time. To avoid common mode failure[4], part of ZC-C's data is not synchronised with ZC-A and ZC-B, which would be re-created in ZC-C upon taking over as the active ZC.

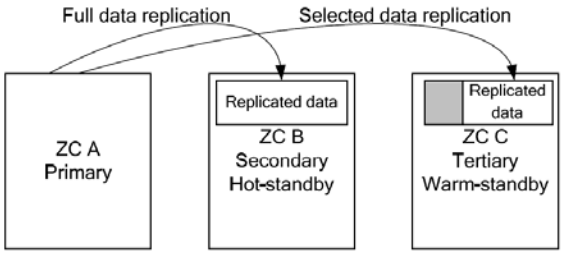


Figure 4: Design functions of the three ZCs

The addition of ZC-C in the new signalling system as warm-standby is a new design and its switch-over mode is more sophisticated than that of conventional design which adopts only two ZCs as active and hot-standby configurations.

[4] Common mode failure means that the same fault occurs at the tertiary warm-standby ZC when it takes over control as the active ZC from the primary ZC and the secondary hot-standby ZC.

3.5 Under all circumstances, only one ZC should be active in the signalling system to control the trains. The active ZC will receive information of operating trains and tracks at all times, including positions, speed, travelling direction and speed limit restriction of the trains at particular sections, points, and crossover positions. Not only does the active ZC calculate and maintain a safe distance between trains, it also restricts the simultaneous entry of more than one train into a point or crossover track to ensure safe railway operation.

3.6 Under normal conditions the active ZC will be either ZC-A or ZC-B. The active ZC regularly sends dynamic data to the warm-standby ZC-C every 100 milli-seconds. In order to minimise common mode failure, based on information extracted from the incident investigation report submitted by the supplier, the following six route-related data items would not be replicated from the active ZC (i.e. either ZC-A or ZC-B) to the warm-standby ZC (ZC-C) (Figure. 5) :

- Conflict zone
- Crawlback
- Crossline
- Border reservation
- Switch control
- Signal control

3.7 In the event when both ZC-A and ZC-B are faulty, the warm-standby ZC-C will act as the active ZC. In handling the route-related conflict zone data, the warm-standby ZC-C will first initialise its internal data space, then call a software subroutine to combine dynamic data collected from the corresponding trackside and signalling equipment with the corresponding static data (which is stored in the ZC-C database) for ZC-C to execute the signalling functions. These dynamic data include :

- Number of conflict zone objects
- Whether the conflict zone has overlapped with non-communicating objects
- Whether the conflict zone has overlapped with non-communicating objects during the previous cycle
- Number of users inside the conflict zone
- Train identification of the user
- Route identification of the user

The above dynamic data of the conflict zone, once collected from the trackside and signalling equipment, will be combined with the following two static data of the conflict zone in ZC-C:

- Conflict zone identification
- Number of paths set in the conflict zone

A complete and correct set of conflict zone data will be re-created based on the above dynamic data and static data for ZC-C to execute the signalling functions, including ATP to prevent train collision in the conflict zone.

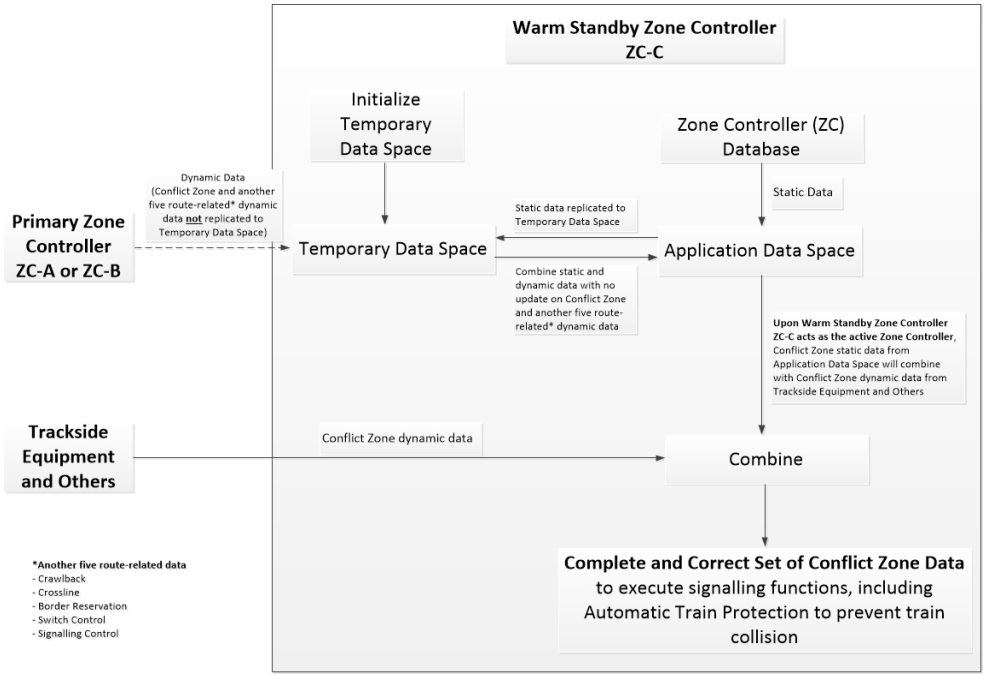


Figure 5: Integration of conflict zone data from primary/secondary ZCs, warm-standby tertiary ZC and trackside equipment

3.8 However, during the collision incident, due to programming error, the software subroutine mentioned above for conflict zone was not executed in the warm-standby ZC-C when it took up the active ZC role, and therefore the conflict zone data in ZC-C could not be re-created correctly. This error allowed two trains to enter the incident conflict zone and caused the collision.

4. Approach of Investigation

4.1 The EMSD conducted an independent, in-depth and comprehensive investigation into the causes of this incident. The EMSD also appointed three independent parties to provide expert advice, namely TPD System Asia Limited (TPDSA), an railway safety consultant with overseas experts in incident investigation, safety management and risk assessment of systems and processes; Professor Roderick Smith of the Imperial College, an expert in railway safety; and Professor Felix Schmid of the University of Birmingham, an expert in railway signalling systems. In carrying out the investigation, the EMSD has:

(a) conducted more than 65 meetings and reviewed over 250 documents and records, which cover 16 different document categories including project contract documents, design documents, testing and commissioning plans, testing and commissioning reports, testing certificates, procedures for drill and exercise, safety certificates, software programming codes, notes of meetings, recommendations from the Independent Safety Assessor (ISA) and the Independent Reviewer (IR) engaged by the MTRCL, traffic notices, safety briefing records, briefing records for drills and exercises, train logs and investigation reports;

(b) reviewed the traffic notices of the OCC, safety briefing records, briefing records for drill and exercise, incident train logs, trainborne signalling logs of the incident trains and ZC alarm logs on the day of the incident;

(c) reviewed the CCTV footage of the platform and concourse areas before and after the incident;

(d) reviewed the software programming versions of the incident ZCs and trainborne signalling equipment as well as conducted simulation tests on the three incident ZCs;

(e) reviewed the corresponding software programming codes;

(f) reviewed the investigation reports of the MTRCL and the ATDJV;

(g) interviewed 106 MTRCL staff, viz. 53 project team staff, 4 OCC staff, 11 station staff and 38 train captains;

(h) interviewed 27 project team staff from the ATDJV;

(i) interviewed 2 representatives from the ISA (Arthur D Little Limited); and

(j) interviewed 2 representatives from the IR (Kusieog Limited).

5. The EMSD Investigation Findings

5.1 Cause of Incident

According to the EMSD's investigation, the new signalling system performed differently from its intended operation as described in paragraph 3.7. On the day of the incident, the MTRCL performed a drill and exercise on site to simulate a failure in the primary and secondary ZCs, which controlled the stations between Central and Sham Shui Po during peak hours. The purpose of the drill and exercise was to train personnel from the MTRCL to cope with this failure. The scenario of the drill and exercise was that the primary ZC (ZC-A) and the secondary ZC (ZC-B) on hot-standby mode failed simultaneously, and that the signalling system had to be switched over to the tertiary ZC (ZC-C) on warm-standby mode to maintain train operation.

The investigation revealed, when ZC-C took up the active ZC role, the computer programme for handling conflict zone data did not execute the relevant subroutine to combine the dynamic data with the static data and did not re-create the conflict zone information correctly (Figure 6). Because the correct information on the conflict zone was not available, the conflict zone at the crossover track at Central Station did not exist in ZC-C. In the end, the ATP system could not function properly to prevent two trains from entering the crossover track simultaneously and resulted in the train collision.

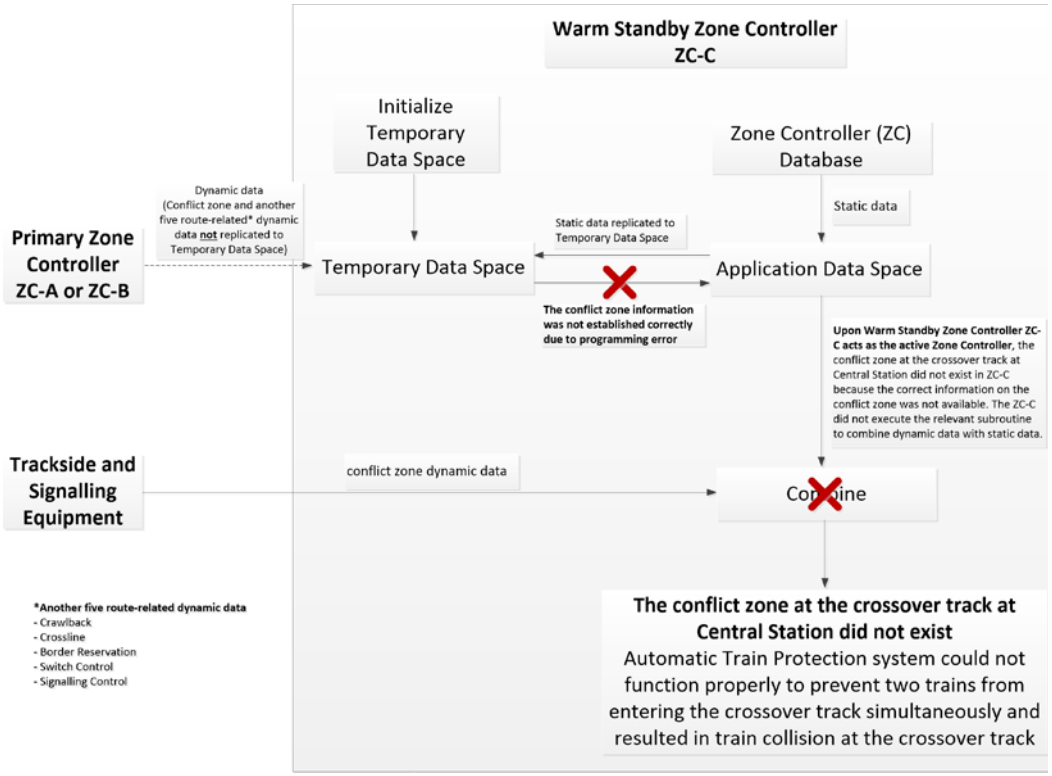


Figure 6: The tertiary ZC did not execute the relevant subroutine to combine the dynamic data with static data

5.1.1 Test items

After the incident, the EMSD and its appointed railway consultant performed multiple tests at the Kowloon Bay Depot, the Ho Man Tin Station[5], the ATDJV Office in Hong Kong and the ATDJV Software Development Centre in Toronto, Canada. The tests were as follows:

(a) Brake tests for the incident trains

A series of brake tests were performed on the incident train T131 at the Kowloon Bay Depot to test the operation of the brake system, with a view to ascertaining whether the incident was related to the brake system of the train. According to the test results, the brake system operated properly and hence was not related to the incident.

(b) Computer simulation tests for the signalling system

Computer simulation tests (Figures 7 and 8) were conducted at the Ho Man Tin Station, the ATDJV Office in Hong Kong and the ATDJV

[5] Ho Man Tin Station is equipped with a new signalling system simulator for training purpose.

Software Development Centre in Toronto by using the same software version as that of the trains in the incident, with the same location and conditions of the incident to ensure that the scenarios were identical. The test results of the simulations revealed that the same collision would happen by using the same software version in the simulators.

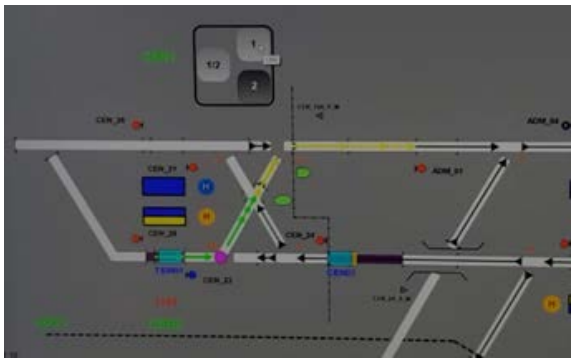


Figure 7: Simulator in ATDJV Hong Kong Office showed the route setting for trains T112 and T131 entering the conflict zone at Central Station at the same time.

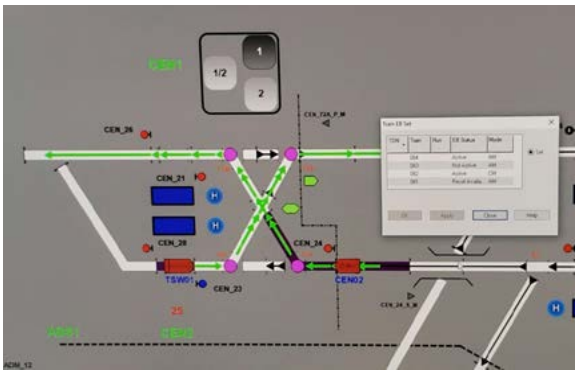


Figure 8: Simulator in ATDJV Hong Kong Office showed the trains entering the conflict zone at the same time at Central Station, as the route setting had allowed them to do so.

(c) Simulation tests for incident ZCs and vehicle on-board controllers (VOBCs)

Simulation tests (Figures 9 and 10) were conducted at Ho Man Tin Station by using the ZCs and VOBCs of the incident trains with the same location and conditions of the incident, with a view to ascertaining whether the incident was caused by the incident ZCs and VOBCs. According to the results of the simulations, the same incident would happen by using the incident ZCs and VOBCs in the simulator.

Figure 9: Simulator in Ho Man Tin Station

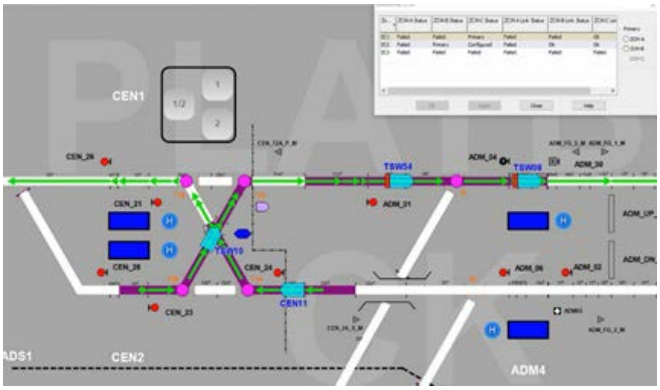


Figure 10: Simulation results showed the ZCs and VOBCs of the incident trains allowing the trains to enter the conflict zone at Central Station at the same time

5.2 Development, Verification and Testing of Signalling System and Drill and Exercise

5.2.1 Programming error in ZC

Investigation showed that there was a programming error in the signalling system software for ZCs after a modification of software coding in July 2017. Due to this programming error, when ZC-C was switched over to become the active ZC, the computer programme for handling conflict zone data did not execute the relevant subroutine to combine the dynamic data with static data, hence the conflict zone at Central Station could not be properly re-created in ZC-C. The ATP system could not function as required to prevent two trains from entering the crossover track at the Central Station at the same time and led to the train collision.

5.2.2 Development process of software programme

It is specified in BS EN 50128 (Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems) that the specification, functional requirements and programming logic of the software should be properly recorded during the development process to allow software developers to formulate relevant tests and reviews in the subsequent verification and validation process. The investigation revealed that the software coding of tertiary controller

ZC-C made in July 2017 regarding the conflict zone data had not been properly recorded in the software design, and therefore the related software coding error was not detected in the subsequent verification and validation process.

This means that the software design and the corresponding change request did not specify how to properly handle the re-creation of conflict zone data in ZC-C. The design and change control documents only mentioned that data related to existing route request, route authorisation and Limit of Movement Authority (LMA) would not be replicated to ZC-C, without mentioning that conflict zone data also would not be replicated to ZC-C. If the software developer had properly recorded all the specifications, functional requirements, programming logic and modifications made in the software, the error codes might have been identified and rectified in the subsequent verification and validation process.

5.2.3 Risk assessment for signalling system

A typical signalling system usually deploys two ZCs (i.e., primary ZC-A and secondary ZC-B) for switch-over between active and hot-standby modes. The provision of tertiary ZC in warm-standby mode in the new Tsuen Wan Line signalling system is a unique implementation by the supplier among the supplier's standard signalling system products. The investigation revealed that risk assessment had not been comprehensively conducted to address the potential hazards due to the unique design of ZC-C during system development. For the design of ZC-C in combining dynamic and static data of conflict zone, if the following activities, including detailed risk assessment, safety requirement identification, verification of safety documents in design documentation, implementation of safety requirements in design, review of design, implementation of the requirements in code, review of the code, and corresponding comprehensive simulation tests or on-site tests had been all properly conducted, the software coding errors might have been identified.

5.2.4 Verification and validation process

In view of the concerns and comments raised by the ISA engaged by the MTRCL, additional verification and validation checking on the software were conducted from October 2018 to February 2019. Most of the additional verification and validation checking were completed on 1 March

2019, but the above-mentioned software coding errors were not identified. The independent software assessment scheduled for February 2019 was not completed as scheduled. If such assessment had been completed in February 2019 as required, the software coding errors might have been identified. However, the EMSD's appointed consultant was of the view that the programming error might still not be identified in the above independent software assessment.

5.2.5 Testing of signalling system

The international standard, IEEE1474.4 (Recommended Practice for Functional Testing of a Communications-Based Train Control (CBTC) System), states that simulation tests to the maximum extent possible should be conducted during the stage of factory acceptance tests. Also that on-site functional tests should include functions of the whole signalling system (i.e. including ZC-C), so as to verify that the CBTC functional requirements are satisfied. According to records, comprehensive simulation tests of conflict route were not conducted for the incident scenario (i.e. both ZC-A and ZC-B failed, with ZC-C switched over to be the active ZC) during the factory functional testing stage and on-site functional testing stage. Had comprehensive simulation tests and on-site functional tests been conducted to the maximum extent possible, the programming error and the issue of the ZC-C being unable to re-create conflict zone data might have been identified.

5.2.6 Simulation of signalling system

The provision of tertiary ZC in warm-standby mode in the Tsuen Wan Line signalling system is a unique implementation by the supplier among the supplier's standard signalling system products. The specific requirements of tertiary ZC in warm-standby mode in signalling system were stipulated in the Particular Specification of the contract document. The design requirement was detailed in system design, which only stated the route request, route authorisation and LMA would not be replicated to ZC-C. If the design documents had covered details on the handling of conflict zone data upon ZC-C taking over as the active ZC, and more comprehensive simulation tests had been conducted for the non-standard design prior to the site tests, the corruption of the conflict zone data at the incident crossover track might have been discovered earlier and rectified and the incident on 18 March 2019 might not have happened.

5.2.7 Arrangement of on-site drills

The MTRCL engaged an ISA to certify the safety of the new signalling system before it is deployed to service. On the basis that the new signalling system was to be commissioned in mid-2019 as earlier planned. The ISA reported to the MTRCL on 19 October 2018 that the weaknesses of the signalling safety assurance system might result in an unsafe incident and improvements were required. The ISA raised the following comments on 6 February 2019 and reiterated the subject on 5 March 2019 that:

(a) they did not believe the signalling system fully complies with recognized international standards;

(b) they had significant concerns on compliance with the system developer's software development processes; and

(c) they did not believe that the development processes employed by the supplier are commensurate with the complexity of the signalling system. Many latent safety anomalies were identified on the system core software (Convergence 3.2) since the issue of the safety certification. These revealed the fundamental process weaknesses. The likelihood that such weaknesses might result in an unsafe incident was unacceptably high.

In response to the ISA's comments, the concerned parties carried out tri-partite workshops on 19-25 February 2019 to discuss the ISA's concerns and the system's development progress. After the meeting, the MTRCL postponed the planned service of the new signalling system by six months to Q4 of 2019 to allow time for the ATDJV to respond to the ISA's concerns and improve the new signalling system. The ATDJV indicated that a new version of the signalling system would be released on 24 May 2019. The new version is Build 8.3.4, whilst the version used in the incident was Build 8.3.3. According to records, both the ATDJV and the MTRCL, who participated in the drills and exercises, were aware of the scheduled release of the new software version in May 2019 and the content of the changes. While the said programming error that led to the incident were identified only after the incident, and was not included in the ATDJV's planned update items of the software in Build 8.3.4, we consider it there might still be a very remote chance that the ATDJV might have identified the programming error in the new build, or during software assessment or review to be conducted

by an independent software team of the ATDJV. Our appointed railway experts were of the view that there was no clear advice at the time that would have triggered the MTRCL to suspend the drills and exercises in the wait for the new software release, and that there was no evidence either the programming error would have been identified and rectified in the new version in any case.

5.2.8 Procedures of on-site drills

Drills and exercises commenced on 16 February 2019. The incident occurred during the 9th drill, in which 34 trains were deployed for on-site drills without making reference to any relevant drill procedures.

6. Investigation Findings of Railway Experts Engaged by the EMSD

6.1 Investigation Findings of Railway Consultant (TPDSA)

6.1.1 The EMSD has already established that the immediate cause of the collision was a software error in the tertiary Zone Controller (ZC-C) used to control the movement of trains prior to the engagement of TPDSA. TPDSA concurs that this is the immediate cause and has investigated the software defect in detail. TPDSA has also performed further investigations to establish why the error occurred and has identified the underlying causal factors as follows:

(a) A relatively brief examination of the software development processes showed significant deficiencies such that an undetected software error remained.

(b) The need of, or benefit from ZC-C has not been demonstrated and diluted the benefits of the proven core-software.

(c) There was no mapping of software requirements or independent review of the requirement interpretation at sub-system level.

(d) Until a late stage, the ISA had voiced out that the software development and safety engineering processes were inadequate and would affect the integrity of the finished product.

(e) The ISA scope was too limited. It did not cover "readiness for testing" either for one, or several trains, even though a Safety Case and Safety Certificate were produced by the supplier.

(f) The management of testing on the railway was poor with informal communication leading to assumptions and confusion as to the limits of testing and therefore insufficient controls applied.

(g) There was a lack of openness within the system contractor organisation and in its communication with the client. Communication broke down such that a PowerPoint presentation was wrongly interpreted as authority to proceed with any drills and exercises, even though the Safety Case and Safety Certificate had limitations.

(h) The Safety Case and Safety Certificate relating to the drills and exercises lacked clarity and traceability and there were gaps in the safety analysis arising from the introduction of the ZC-C such that compliance with EN50129 (Railway applications -Communication, signalling and processing systems - Safety related electronic systems for signalling) was not achieved.

(i) Programme and commercial pressures to start testing overtook the need for robust process to achieve correct software, the importance of which might not have been fully understood by the parties involved.

(j) The significance of latent safety defects identified in the core software and safety restrictions imposed on it were not understood as a precursor to poor process and therefore poor software. Decisions were made based on assumptions about the dependability of the core software that were shown to be unfounded.

(k) The operational staff (Traffic Controllers and Train Captains) could not reasonably have been expected to have done any more to prevent or mitigate the incident.

(l) The independent software assessment team is considered not sufficiently independent although they are from another unit of the supplier.

(m) The EMSD was kept at a distance in their regulatory role despite regular meetings. The difficult issues, such as the emerging ISA findings were not shared with the EMSD.

6.1.2 In summary, the requirement management, engineering safety management and software development processes were not in accordance with international standards EN50128 and EN50129, which were specified in the contract and are proven internationally for signalling systems. This led to an undetected error in their software.

6.1.3 A contributory cause was that warnings from the ISA that the software could not be relied on, were not fully resolved before the incident. In addition, the ISA remit did not cover "readiness for testing" even though a Safety Case and Safety Certificate were produced. The ISA's limited remit led to a situation where un-validated software without adequate safety controls was used for the drills and exercises for testing.

6.2 Investigation Findings of Professor Roderick Smith

6.2.1 The incident was caused by a weakness in the controlling software which failed to perform the necessary handshake of information when a test was performed to simulate the failure of the first two controllers. It is considered as a sound conclusion agreed by all related parties. This major conclusion is supported without reservation.

6.2.2 Doubts had been expressed by the ISA as early as October 2018 which were repeated in 6 February and 5 March 2019. These doubts contained comments such as lack of belief that the system fully complied with international standards and "latent anomalies" contained in the software might result in an unacceptably high risk of an unsafe incident. There followed tri-partite workshops between 19-25 February 2019 after which the introduction of the new system into revenue service was postponed to Q4 of 2019. This was the fourth of a series of push-backs from the original target of May 2018. This is very clear evidence that all parties were aware of difficulties arising from the testing prior to service introduction of this new system. A new version of the software was promised for May 2019. Between 16 February and the incident on 18 March eight further testing drills were conducted without any problems arising. At the time of the incident on 18 March, 34 trains were involved. There was no clear advice

issued by any party to the project proponent outlining the circumstances in further tests which would lead to unacceptable risk, nor any instruction to suspend testing until the new software became available.

6.2.3 Software has become increasingly complex and is being used in a huge variety of situations. It is difficult, perhaps impossible, to test complex software off-line for all eventualities. The authorship of such software is generally a team effort over a considerable period of time and many versions. Ensuring continuity is extremely difficult. The modelling of testing scenarios is only as good as the imaginations of the authors of the risk assessments prior to service introductions. There must be an element of reduction of probabilities in the testing and acceptance of software: a reduction of risk as far as reasonably practical is the goal and this will never be 100%. In this case new ground was being broken by the new signalling system.

6.3 Investigation Findings of Professor Felix Schmid

6.3.1 The significance of implementing a warm-standby rather than a hot- standby configuration in order to reduce the risk of a “data-driven” common-mode failure of all three ZCs, was not clearly understood by the stakeholders. In fact, the warm-standby system with three Zone Controllers A, B and C is a unique and non-standard design among its standard signalling system products of the supplier, which was requested specifically by the MTRCL to satisfy their exacting availability targets.

6.3.2 Individually, both the implementation of a CBTC system on an existing operating railway, and the introduction of a tertiary ZC-C would be deemed major changes. The criticality of combining the two changes was not recognized by the stakeholders.

6.3.3 The non-replication of conflict zone data to tertiary ZC-C should have been detailed in the system design document and in the subsequent formulation of simulation and field testing.

6.3.4 The non-replication of conflict zone data to tertiary ZC-C is not detailed in the system design document. Hence in addition to the programming (logic) omission, the poor system design documentation, the inadequate formulation of simulation and field testing were contributing factors.

7. Conclusions

Based on the investigation findings of the causes of the incident, the EMSD concludes that the train collision incident at the crossover track at the Central Station on Tsuen Wan Line during the drill and exercise in non-traffic hours on 18 March 2019 was due to the following reasons:

(a) there was a programming error in the software of the warm-standby tertiary ZC involved in the incident, resulting in a failure to re-create conflict zone data of the crossover track at the Central Station after switch-over from the primary ZC to the warm-standby tertiary ZC. Hence, the ATP system could not function as required to prevent two trains from entering the crossover track at the Central Station at the same time and led to the train collision;

(b) the programming error, which was introduced in July 2017 during software rectification of the new signalling system, was not identified by the system contractor during various system testing / software upgrades as a result of poorly specified design requirements and inadequate verification and validation processes of the software;

(c) the potential risk arising from the introduction of the warm-standby tertiary ZC was not comprehensively included in the risk assessment by the system contractor for the new signalling system; and

(d) simulation tests were not conducted to the maximum extent by the system contractor prior to the site tests, taking into account the specific requirement for a warm-standby tertiary ZC, which is a unique implementation by the supplier among the supplier's standard signalling system products.

8. Measures Taken after the Incident

8.1 Subsequent to the collision incident, the MTRCL has suspended all testing of the new signalling system on the Tsuen Wan Line, Island Line and Kwun Tong Line immediately. The MTRCL has also announced that all train tests for the new signalling system during non-traffic hours would continue to be suspended until the root cause of the incident has been identified.

8.2 The EMSD notes that the MTRCL Investigation Panel has made a number of recommendations to the system contractor and the MTRCL, and agrees that such recommendations aim to rectify the programming error and enhance the development and testing process of the new signalling system, with a view to preventing recurrence of similar incident. The EMSD will monitor the MTRCL's full implementation of the measures and assess the effectiveness of such. The Government will only allow the MTRCL to resume train testing of the new signalling system after the MTRCL has fully completed the remedial work and the EMSD has confirmed the safety of the new signalling system upon inspection.

- End of Report -

Appendix I – Drills and Exercises from 16 February to 18 March 2019

Date	Drills and Exercises
16 Feb 2019	Drills and Exercises No. 1 Simulate points machine failure and train fault
21 Feb 2019	Drills and Exercises No. 2 Simulate OCC blackout, OCC evacuation and other operational exercise
23 Feb 2019	Drills and Exercises No. 3 Simulate Smart I/O failure and assisting train
28 Feb 2019	Drills and Exercises No. 4 Simulate power supply failure and docking failure
9 Mar 2019	Drills and Exercises No. 5 Simulate power supply failure and docking failure
12 Mar 2019	Drills and Exercises No. 6 Simulate Smart I/O failure
15 Mar 2019	Drills and Exercises No. 7 Simulate OCC blackout, OCC evacuation and other operational exercise
17 Mar 2019	Drills and Exercises No. 8 Simulate assisting train
18 Mar 2019 (Date of incident)	Drills and Exercises No. 9 Simulate ZC failure

Appendix II – Sequence of Events

Time	Description
18 March	
0:15 a.m.	The ATDJV conducted briefing to the MTRCL staff, followed by briefing to the MTRCL staff by the MTRCL's drills and exercises in-charge.
2:44 a.m.	Two trains collided at Central Station.
2:54 a.m.	The Fire Services Department and Hong Kong Police Force were notified of the incident. The two train captains were sent to the hospital for medical check, and were discharged on the same day.
2:56 a.m.	The Transport Department (TD) was informed of the incident.
3:03 a.m.	The EMSD was informed of the incident.
3:17 a.m.	The TD was informed regarding the service disruption of Tsuen Wan Line.
4:00 a.m.	"Red alert" issued by the MTRCL. Passengers were informed of the Tsuen Wan Line service disruption through Traffic News and the media. Train service between Admiralty Station and Central Station of Tsuen Wan Line was temporarily suspended.
19 March	
Full Day	Recovery works in progress.
11:00 p.m.	Two bogies of one of the trains were re-railed.
20 March	
0:00 a.m. to 1:15 a.m.	Recovery works in progress.
1:15 a.m.	The trains were moved to the sidings of Admiralty Station and safety inspection was conducted after completion of the recovery works.

Appendix III – EMSD's views on the MTRCL Investigation Panel Report

There is no conflict on the investigation findings between the EMSD Investigation Report and the MTRCL Investigation Panel Report. Nevertheless, the EMSD considers the other facts and factors below are relevant to the incident:

(a) The provision of tertiary ZC in warm-standby mode is a unique and non-standard design among its standard signalling system products of the supplier, as such comprehensive risk assessments should be taken by the supplier and should not be limited by the software development document; and

(b) The simulation tests for the tertiary ZC during the stage of the factory acceptance tests could have been conducted comprehensively by the supplier because of its unique and non-standard design. The scope of simulation tests for tertiary ZC should make reference to IEEE1474.4 be of maximum extent and should not be limited by the software development document.

Besides, the MTRCL's Investigation Panel Report mainly focused on the deficiencies of the supplier in software development and system implementation processes. The Report did not mention the roles of the MTRCL Operations Project Team in overseeing the project implementation. The EMSD considers that, having regard to the significance of this project and the fact that the system design being a non-standard one, the MTRCL should avoid over-reliance on the contractor but ought to be extra vigilant at all times.

The EMSD also notes in the MTRCL's Investigation Panel Report that the Panel has recommended the ATDJV and the MTR Operations Project Team to implement a number of improvement measures to rectify the programming error and enhance the development process of the new signalling system (including the testing), with a view to preventing recurrence of similar incident. Specifically, the MTRCL has undertaken to –

(a) expand the scope of the ISA from safety assurance for passenger service to the inclusion of on-site train-related testing certification;

(b) upgrade the Training Simulator in Hong Kong to act as a testing simulation tool to perform more scenario simulation tests as far as practicable;

(c) establish a joint safety Test & Commissioning Panel (MTRCL/ATDJV together with input from the ISA) to manage on-site testing; and

(d) explore together with the Panel's experts on the merits, if any, for staging the development of the warm-standby computer, or any other technically appropriate alternatives proposed by the ATDJV.

The EMSD will monitor the MTRCL's full implementation of the measures and assess the effectiveness of such. The Government will only allow the MTRCL to resume train testing of the new signalling system after the MTRCL has fully completed the remedial work and the EMSD has confirmed the safety of the new signalling system upon inspection.

Confidential

Investigation Panel Report on Train Collision Incident at Central Station (Tsuen Wan Line) during Non-traffic Hours on 18 March 2019

Submitted by:

Adi Lau	Peter Ewen
Operations Director	**Engineering Director**

Investigation Panel Co-Chairpersons

Date: 17 June 2019

Table of Contents

Executive Summary

1. Introduction

2. The Investigation Panel

3. Background

   3.1 Signalling Replacement Project

   3.2 Testing and Simulation

   3.3 Safety Assurance

4. The Incident

5. Causes of the Incident

6. Findings

7. Conclusions

8. Recommendations

Annex 1 Overall Programme of Simulations and Testing

Annex 2 Illustration of the Scenario

Annex 3 Data Transfer among the Three Computers A, B and C

Executive Summary

During the non-traffic hours on 18 March 2019, a drill was conducted on the new signalling system provided by the contractor Alstom-Thales DUAT Joint Venture (ATDJV) on the Tsuen Wan Line (TWL). The objective of the drill was to familiarize the operators with the system behaviour and the application of operational procedures in a situation in which both the Primary and Hot-standby computers failed and there was a need to switch to the Warm-standby computer.

At around 02:44 hours, a non-passenger train which was heading to a platform of Central Station (CEN) through a crossover collided with another non-passenger train that was departing from CEN for Admiralty Station (ADM) through the same crossover, causing damage to both trains. Both Train Captains were sent to hospital for medical checks, and they were discharged on the same day.

The Corporation was greatly concerned about the incident and therefore set up an Investigation Panel with membership consisting of MTR senior personnel and external experts to investigate and identify the cause of the incident, and make recommendations to prevent the recurrence of similar incident.

The investigation concluded that ATDJV had created a software issue which led to the missing of conflict zone protection at the crossover, resulting in the aforementioned two trains being allowed to enter into and collide at the crossover. The software issue was created as a result of software implementation errors made during the process of performing a software change.

The Panel further concluded that the software implementation errors reflected inadequacies in ATDJV's software development process with respect to software quality assurance, risk assessment and the extent of simulation on this software change.

Recommendations were made by the Panel to ATDJV to:

(a) replace the software design and development team causing the software issue;

(b) fix the software change issue and confirm with substantiation that there are no wider implications in software development quality;

(c) enhance the software coding and testing practices to avoid future programming errors and introduce effective and traceable measures for detection of any programming errors; and

(d) develop a full range of effective measures, including but not limited to (i) employing an external Independent Software Assessor to enhance the software development process for Computers A/B and C from its core product; (ii) reviewing, re-checking and demonstrating robustness on its approach with traceable evidence in applying a fail-safe principle; and (iii) conducting risk assessment in its software implementation with support from the Panel's experts.

To assist ATDJV to address the above, the Panel recommended the MTR Operations Project Team to exercise extra vigilance and strengthen the monitoring on ATDJV's deliveries to rebuild public confidence as below:

(a) expand the scope of the Independent Safety Assessor (ISA) from safety assurance for passenger service to the inclusion of on-site train-related testing certification;

(b) upgrade the Training Simulator in Hong Kong to act as a testing simulation tool to perform more scenario simulation tests as far as practicable;

(c) establish a joint safety Test & Commissioning Panel

(MTR/ATDJV together with input from the ISA) to manage on-site testing; and

(d) explore together with the Panel's experts on the merits, if any, for staging the development of the Warm-standby computer, or any other technically appropriate alternatives proposed by ATDJV.

Only with consent obtained from the Government, will train testing of the new signaling system during non-traffic hours be allowed to resume.

1. Introduction

1.1 At around 02:44 hours of 18 March 2019, which was during non-traffic hours, a drill was conducted on the new signalling system on the Tsuen Wan Line (TWL). A non-passenger train which was heading to a platform of Central Station (CEN) through a crossover, collided with another non-passenger train that was departing from CEN for Admiralty Station (ADM) through the crossover at the same time, causing damage to both trains.

2. The Investigation Panel

2.1 The Corporation was greatly concerned about the incident and therefore set up an Investigation Panel to investigate and identify the cause of the incident, and make recommendations to prevent the recurrence of similar incident.

2.2 The Panel was chaired jointly by Adi Lau, Operations Director and Peter Ewen, Engineering Director. Membership consisted of senior MTR personnel in the fields of Operations and Engineering as well as external experts, namely Gab Parris, Peter Sheppard and Joseph Wong of a globally recognized engineering consulting firm WSP, and Prof. S.L. Ho, the Associate Vice President (Academic Support), The Hong Kong Polytechnic University.

3. Background

3.1 Signalling Replacement Project

3.1.1 Signalling systems are essential for safe operation of train services in railway networks. To increase train frequency and capacity as well as to progressively replace the existing assets, in January 2015 MTR awarded a competitively tendered contract for the replacement of the signalling systems on seven railway lines (Tsuen Wan Line, Island Line, Kwun Tong Line, Tseung Kwan O Line, Disneyland Resort Line, Tung Chung Line and Airport Express). The contract was awarded to Alstom-Thales DUAT Joint Venture (ATDJV), a joint venture between Alstom Hong Kong Limited (Alstom) and Thales Transport & Security (Hong Kong) (Thales). Both Alstom and Thales are internationally renowned railway infrastructure suppliers having proprietary rights and knowledge over their products and technology.

3.1.2 The TWL signalling system is divided into two control zones. In each control zone, the new signalling system comprises three signalling zone controller computers as required by the contract, namely Computer A as the Primary Computer, Computer B as the Hot-standby computer and Computer C as the Warm-standby computer. Computers A, B and C are of the same hardware and loaded with common software. They are configured to perform functions of Computers A, B and C through a hardware identity plug which allows the common software to process dynamic data among the three computers correspondingly. Computer C only receives selected dynamic data from Computers A/B so as to avoid common mode failure. This configuration aims to improve system availability and service recovery through higher resilience. The Warm-standby arrangement is novel in ATDJV's signalling system application. Furthermore, Computer C is housed at a different station which enhances system security through access control and diverse power supply.

3.2 Testing and Simulation

3.2.1 The MTR Operations Project Team managed the replacement work by applying a method widely adopted in the railway signalling industry. This method, which was implemented by the contractor, included software simulation testing in its laboratory and on-site testing to ensure the new signalling system was developed and matured in a safe and controlled manner. All related testing activities were conducted in a step-by-step and incremental approach along key stages with certification protocols and safety documentation issued by ATDJV. The diagram at Annex 1 shows the overall programme of the simulations and testing.

3.2.2 ATDJV started on-site train testing during non-traffic hours on TWL in December 2016 and the scope of test was progressively extended from one train to multiple trains.

3.2.3 Through stage-by-stage system maturity testing, incremental confidence was built up on the readiness of the new signalling system to start drills on the system operation and operator familiarization of the system behaviour in February 2019. The drills were jointly performed by the MTR Operations Project Team and ATDJV.

3.2.4 Based on the previous simulations, which had been conducted with the common software installed on all computers while not repeating in Computer C for the completed simulations done on the common software, and also testing of its specific transition function from Computer A/B to C, ATDJV issued related safety documentations giving the MTR Operations Project Team the confidence in allowing Computer C to become the Primary Computer for the drill. The objective of the drill was to familiarize the operators with the system behaviour. Through the drill, the operators would have the opportunity to become conversant with the multitude of train service situations expected in future day-to-day operations. The drill would also enable fine-tuning of the operational procedures if required before the new signalling system is eventually put into passenger service.

3.3 Safety Assurance

3.3.1 ATDJV has the responsibility to supply a safe signalling system in accordance with the contractual obligations and design requirements. The MTR Operations Project Team required ATDJV to define the scope and the extent of simulations and tests to ensure that a safe signalling system is delivered in accordance with international standards per their responsibility.

3.3.2 ATDJV had a project safety team for vetting and certifying software safety for the on-site testing and drills. Besides, they also separately deployed an independent safety team to assess and certify the system safety before the new signalling system would be certified for passenger service.

3.3.3 In addition to the ATDJV safety assurance described above and to further ensure the safety of the new signalling system before it is put into passenger service, the MTR Operations Project Team also appointed an Independent Safety Assessor (ISA) which was tasked to assess the system safety assurance processes followed by the contractor, and to provide a safety endorsement document upon satisfactory assessment of such processes. The ISA was for certification of passenger service only, but not on other earlier key project stages such as commencement of drills. Furthermore, the MTR Operations Project Team appointed an external Independent Reviewer (IR) to provide advice on project implementation risks associated with the operating railway. The ISA and IR were involved in project activities within their own scope of works as described above but neither of their mandates covered the assessment of drills.

4. The Incident

4.1 During the non-traffic hours on 18 March 2019, the MTR Operations Project Team jointly with ATDJV engineers performed the pre-planned drill to verify the handling procedures for coping with the failure of both Computer A and Computer B, thereby leading to Computer C taking over as the Primary Computer. The objective of the drill was to familiarize the operators with the system behaviour and application of

operational procedures when there are Computer failures.

4.2 At around 02:34 hours, Computers A and B were switched off sequentially to simulate the failure and Computer C took over as the Primary Computer as per the system design. All routes that had been set for trains were cancelled and all trains were stopped as expected in the switchover to the Warm-standby Computer C. The Traffic Controller (TC) in the Operations Control Centre (OCC) then had to give "Depart" commands to depart the trains one after another according to normal operational procedures to allow the resumption of train movement.

4.3 At around 02:41:32 hours, the TC gave a "Depart" command to the train berthing at CEN platform 2 in accordance with the procedure. The route for the train to go to ADM platform 1 was then set by Computer C. At around 02:43:53 hours, for normal traffic regulation, the TC disengaged the platform sequencing selection for CEN to allow the waiting train to berth at CEN platform 1 which was vacant. At around 02:44:01 hours, Computer C erroneously set conflicting routes with signal clear, causing the two trains departing within seconds in Automatic Mode to collide at the crossover outside CEN. For such an instantaneous and unexpected system behaviour, it was very challenging and difficult for the TC to respond and intervene at OCC level through the execution of command steps in calling the emergency brake of the trains in time, as the role of the TC was to manage train regulation activities and as such they would not be expected to be checking for and reacting to such unexpected system behaviour. Similarly, although the Train Captain of the train travelling to CEN platform 1 did activate the emergency brake when he saw the train travelling from CEN platform 2 to ADM platform 1, the train was not able to stop before colliding.

The diagram at Annex 2 illustrates the scenario.

4.4 Apart from one of the two Train Captains who had his right knee mildly abraded, none of the MTR staff or ATDJV staff were injured. Both Train Captains were sent to hospital for medical checks, and they were discharged on the same day.

5. Causes of the Incident

5.1 Computers A, B and C were identical in hardware and loaded with the common software but had different identity hardware plugs to configure them to initially perform as Primary, Hot-standby and Warm-standby, i.e. Computers A, B and C respectively. Before June 2017, the data transferred from Computer A to B or from Computer B to C were all identical which meant that any data corruption causing a failure in Computers A and B would be transferred into C creating a common mode failure.

5.2 To avoid common mode failure according to the contract requirement, ATDJV thus initiated a software change in July 2017. Some dynamic data was selected to be excluded (including "Conflict Zone Data" which prevents conflicting routes from being set) from the data transferal from Computer A/B to Computer C, and those excluded data should subsequently be re-created internally in Computer C. The amount of data excluded and re-created was determined by ATDJV with due consideration to the risk of common mode failure and the swift recovery time so required for Computer C to take up as the Primary Computer in case both Computer A and B fail. However, this software change initiated by ATDJV gave rise to a software issue due to a series of software implementation errors made by its software design and development team during the process of performing this software change.

5.3 Investigation revealed that ATDJV had created the software issue which was caused by the following three software implementation errors made during the process of performing this software change. First, while "Conflict Zone Data" was meant to be excluded, out of expectation it was not specified in ATDJV's internal software development document. Because of this lack of specification, no subsequent specific test, risk assessment and safety analysis, including laboratory verification simulation and on-site testing, was done by ATDJV to verify the "Conflict Zone Data" when Computer C took over as the Primary Computer. This was the first software implementation error.

5.4 Second, ATDJV excluded the transfer of the "Conflict Zone Data" from Computer A/B to Computer C, but its software design and development team made a software implementation error in failing to properly re-create the "Conflict Zone Data" internally in Computer C. This second software implementation error resulted in there being no "Conflict Zone Data" when Computer C took over as the Primary Computer.

5.5 Third, the software logic so built by the software design and development team did not stop Computer C from taking over as the Primary Computer when "Conflict Zone Data" was not available; in other words Conflict Zone protection was not available. This is considered as a software implementation error in not implementing appropriate programming logic to prevent Computer C from taking over as the Primary Computer while having no conflicting route protection.

6. Findings

6.1 The Panel found that until the incident, ATDJV was not aware of the software issue as described in Section 5 throughout its verification and validation process, including simulations done as per their process. As the said software issue was not identified by ATDJV, it was therefore not revealed to the MTR Operations Project Team either. The Panel also noted that ATDJV had issued related safety documentation giving the MTR Operations Project Team the confidence that Computer C would be safe for drills. Indeed, since 15 October 2018, there was no restriction on the number of trains used and no restriction on train separation distance required for on-site testing, in accordance with the safety documentation issued by ATDJV. Furthermore, tests had been undertaken with a procedure that allowed Computer C (as Warm-standby) to become the Primary Computer since mid-October 2018, i.e. with Computer C in full control of the system after switching over continuously. Therefore, for any on-site testing from that point, the software issue could have emerged inadvertently if Computer C had taken over as the Primary Computer, depending on the combination of many permitted and probable situational factors. The Panel

opined that the three software implementation errors made during the process of performing this software change before the incident by ATDJV were the causes of the incident.

> ***"WSP's Independent Expert Team considers that ATDJV is responsible for providing assurance to MTR that their product is safe.***
>
> ***With respect to MTR's Drills / Exercises, it is clear that those activities are purely designed to allow MTR to develop and test their operational rule book and familiarize their staff with normal and degraded mode behavior in addition to gaining confidence in the operability and reliability of the 3036 CBTC system."***
>
> ***WSP***
> ***External Expert***

6.2 The Panel also considered that the software implementation errors reflected inadequacies in ATDJV's software development process with respect to software quality assurance, risk assessment and the extent of simulation on this software change.

6.3 The Panel considered that it is the responsibility of ATDJV to formulate the extent of simulations in verifying and validating the common software installed to Computers A, B and C for performing their intended functions. ATDJV should develop the software to the required maturity through their verification and validation process. Simulations to the extent required as per their process had been done as defined in the software development document by ATDJV before the commencement of

on-site testing. Thereafter, extensive on-site testing was conducted, and iterative simulations and testing, with extra time of more than one year given, had been carried out as appropriate in building up the software maturity. Without knowing the software issue and given the results of the simulations and on-site testing conducted including switchover from Computer A/B to Computer C as witnessed by the MTR Operations Project Team, the project moved to the next stage on the basis that the software should have the maturity to allow safe execution of drills for the operators to safely familiarize themselves with the system behaviour in whatsoever operational circumstances, which was allowed as confirmed by the safety documentation provided by ATDJV. Nevertheless, the Panel opined that given the nature of the software change as revealed after the incident, a wider extent of simulation should have been formulated by ATDJV to cover possible impacts to the critical system performance even if changes were not specified clearly in the software development document.

6.4 The MTR Operations Project Team was aware that there would be a further software version to come after the drills. However, the Panel opined that there was nothing to suggest that the drills on 18 March 2019 should be withheld as the maturity of the software already in use should have been sufficient for the purpose as described in paragraph 6.3.

"It would be unreasonable for MTR to make a unilateral decision, based on no solid grounds, to suspend any drills on Build 8.3.3 and wait for the release of Build 8.3.4."

Professor S.L. Ho
External Expert

> ***"According to Thales' documentation provided (i.e. Safety Cert and SOR), it was safe to run the drill on 18th March 2019."***
>
> ***WSP***
> ***External Expert***

6.5 In the process of maturing the software, laboratory simulations had been done by ATDJV to verify the system functions were fit for on-site testing. In relation to the drills, their purpose was for the operator to have site familiarization on the system behaviour and to respond to a multitude of possible in-situ scenarios that can be experienced in real-life operations. With the understanding that the required scenario as defined by the software development document, including switching over from Computer A/B to C had been carried out before arranging the drill, the Panel opined that additional situational case scenarios could still be further included in the simulations to enhance the level of assurance.

6.6 The Panel noted that according to the original resource plan, the procedure for the drill on 18 March 2019 was planned with 4 trains. Yet, there was no longer any limitation on the number of trains according to the safety documentation issued by ATDJV at the time of the drill. In order to represent the morning peak scenario, the MTR Operations Project Team instead informed ATDJV on a number of occasions through the Commissioning Plan that they were to run 34 trains instead of 4 trains on 18 March 2019. The drill was subsequently jointly performed with 34 trains by the MTR Operations Project Team and ATDJV. Since there was no restriction in train separation distance under the procedure, and given the non-existence of conflicting route protection, the incident could have occurred with 2 trains or more as verified during the investigation. The Panel was therefore of the opinion that while the running of 34 trains resulted in raising the likelihood of revealing the unknown software issue, it was

definitely not the cause of the incident. The Panel also noted that the operators participating in the drill acted properly in accordance with the normal operational procedures for handling the scenario that would be encountered in future day-to-day operations.

6.7 The Panel has reviewed the findings and recommendations that the ISA provided previously in relation to their concerns on i) compliance with Thales' internal development processes, ii) full compliance with international standards, and iii) development process weakness and its associated risks in their core product. The Panel noted that the MTR Operations Project Team and the ISA had taken additional measures in the form of extra assessments involving a series of factory visits and extra simulation tests, with extra time of more than one year given to ATDJV, in building up the software maturity and addressing the above ISA's concerns. While noting that the ISA's findings and recommendations were for passenger service and not for drills and testing as per its remit, ATDJV did make progress in closing some findings but not yet all before the incident . The Panel has confirmed with the ISA that, based on their findings thus far, they had not identified any specific issues for cessation of the on-site tests or drills. The Panel hence concluded with due consideration on the ISA's findings and recommendations that there were no specific unsafe issues identified by, nor recommendations from, the ISA to suggest discontinuing on-site testing or drills. Nevertheless, the Panel opined that the MTR Operations Project Team should exercise extra vigilance in addressing the ISA's comments in monitoring ATDJV's deliveries in future.

6.8 The Panel opined that there was no reason to discontinue the on-site testing, including drills based upon the required safety documentation supplied by ATDJV, at the time when the incident happened. Nevertheless, the Panel opined that the MTR Operations Project Team should in future be more vigilant in assessing implications of the ISA's concerns on drills and consider expanding the ISA's scope to cover assessment of on-site testing.

"WSP Independent Expert team (in MTR's place) would have also allowed the Drills to go ahead on the basis that the required safety assurance documentation had been produced by Thales specifically for the Drills and Tests (Specific Application Safety Case with restrictions (SOR) further amended by a Safety Memo), which was underpinned by the incremental assurance and confidence gained from all previous activities and documentation produced."

WSP
External Expert

"MTR had been taking a prudent and incremental approach to gain confidence in the organization of the Tests and Drill & Exercises. Additional steps had also been taken upon receipt of the advices from the Independent Safety Assessor. Hence it was reasonable for MTR to believe the Drill on 18 March should be a routine familiarization exercise."

Professor S.L. Ho
External Expert

7. Conclusions

7.1 The Panel has reviewed the facts and factors relevant to the causes of the incident, and concluded that ATDJV had created the software issue as a result of the following three software implementation errors made during the process of performing this software change.

(a) software development document did not specify the exclusion of the "Conflict Zone Data" which led to no ensuing specific test and safety analysis to identify the unknown software issue;

(b) a software implementation error led to no re-creation of proper "Conflict Zone Data" internally in Computer C when Computer C took over as the Primary Computer; and

(c) while Conflict Zone protection was not available, subsequently Computer C still continued its process to become the Primary Computer because the software logic was so built that it did not stop Computer C from taking over as the Primary Computer, resulting in missing the conflicting route protection.

7.2 The Panel also concluded that the software implementation errors reflected inadequacies in ATDJV's software development process with respect to software quality assurance, risk assessment and the extent of simulation on this software change.

7.3 With ATDJV's weakness as set forth in paragraph 7.2, the Panel also concluded that the MTR Operations Project Team should exercise extra vigilance and additional monitoring measures on ATDJV's deliveries in future.

8. Recommendations

8.1 The Panel has made recommendations based upon on the causes and the lessons learnt from the incident.

8.2 To prevent recurrence of similar incident due to the same causes, the Panel recommended ATDJV to:

(a) replace the software design and development team causing the software issue;

(b) fix the software change issue and confirm with substantiation that there are no wider implications in software development quality;

(c) enhance the software coding and testing practices to avoid future programming errors and introduce effective and traceable measures for detection of any programming errors; and

(d) develop a full range of effective measures, including but not limited to (i) employing an external Independent Software Assessor to enhance the software development process for Computers A/B and C from its core product; (ii) reviewing, re-checking and demonstrating robustness on its approach with traceable evidence in applying a fail-safe principle; and (iii) conducting risk assessment in its software implementation with support from the Panel's experts.

8.3 To assist ATDJV to address the above, the Panel recommended the MTR Operations Project Team to exercise extra vigilance and strengthen the monitoring on ATDJV's deliveries to rebuild public confidence as below:

(a) expand the scope of ISA from safety assurance for passenger service to the inclusion of on-site train related testing certification;

(b) upgrade the Training Simulator in Hong Kong to act as a

testing simulation tool to perform more scenario simulation tests as far as practicable;

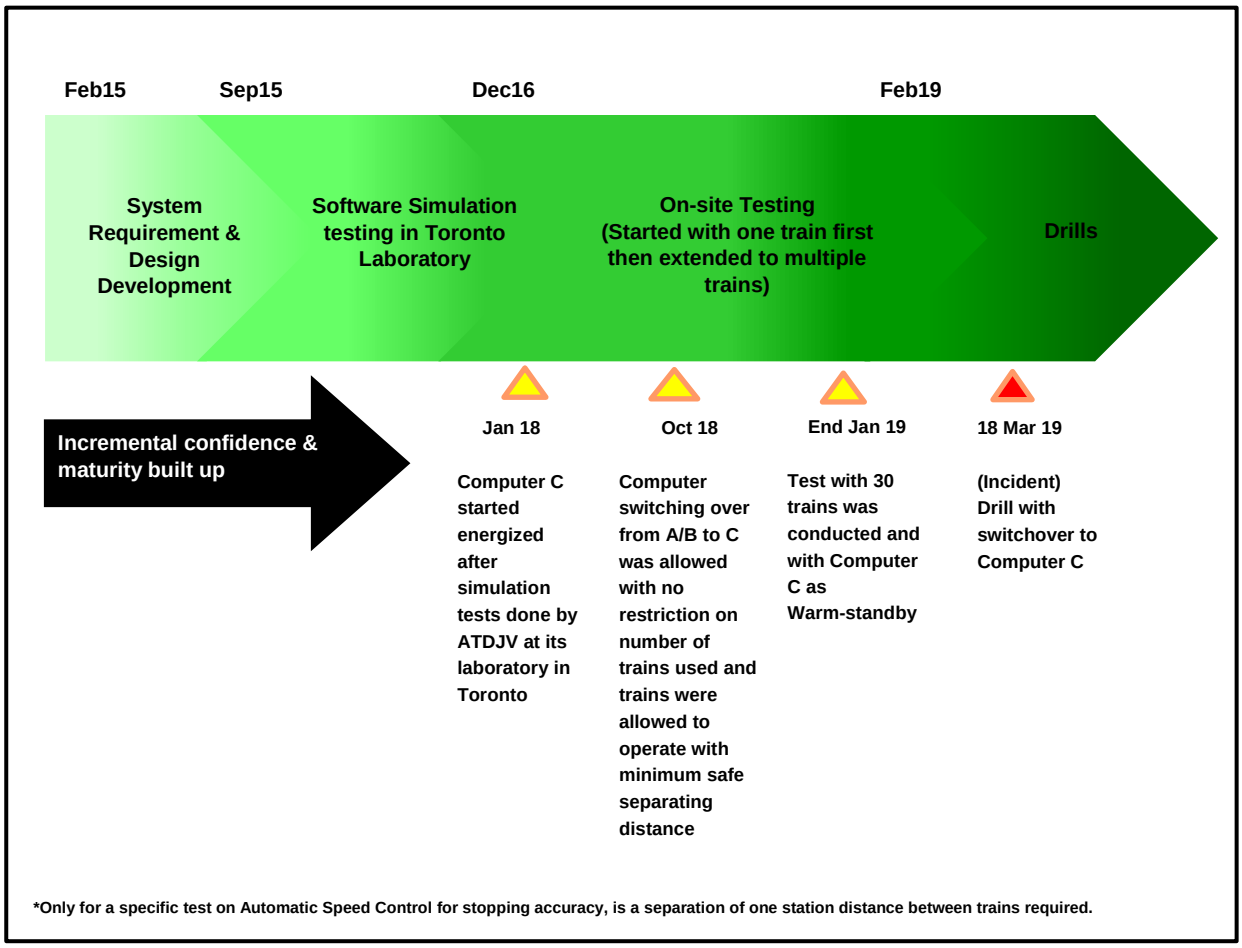
(c) establish a joint safety Test & Commissioning Panel (MTR/ATDJV together with input from the ISA) to manage the on-site testing; and

(d) explore together with the Panel's experts on the merits, if any, for staging the development of the Warm-standby Computer C, or any other technically appropriate alternatives proposed by ATDJV.

8.4 Only with the consent obtained from the Government, will train testing of the new signalling system during non-traffic hours be allowed to resume.

Annex 1

Overall Programme of Simulations and Testing



Notable activities

1. ATDJV started on-site train testing during non-traffic hours on TWL in December 2016 and the scope of test was progressively extended from one train to multiple trains.

2. In January 2018, Computer C started to be energized as Warm-standby after simulation tests done by ATDJV at its laboratory in Toronto.

3. From 15 October 2018 onwards, in accordance with the safety documentation issued by ATDJV, computer switching over from A/B to C was allowed with no restriction on the number of trains used

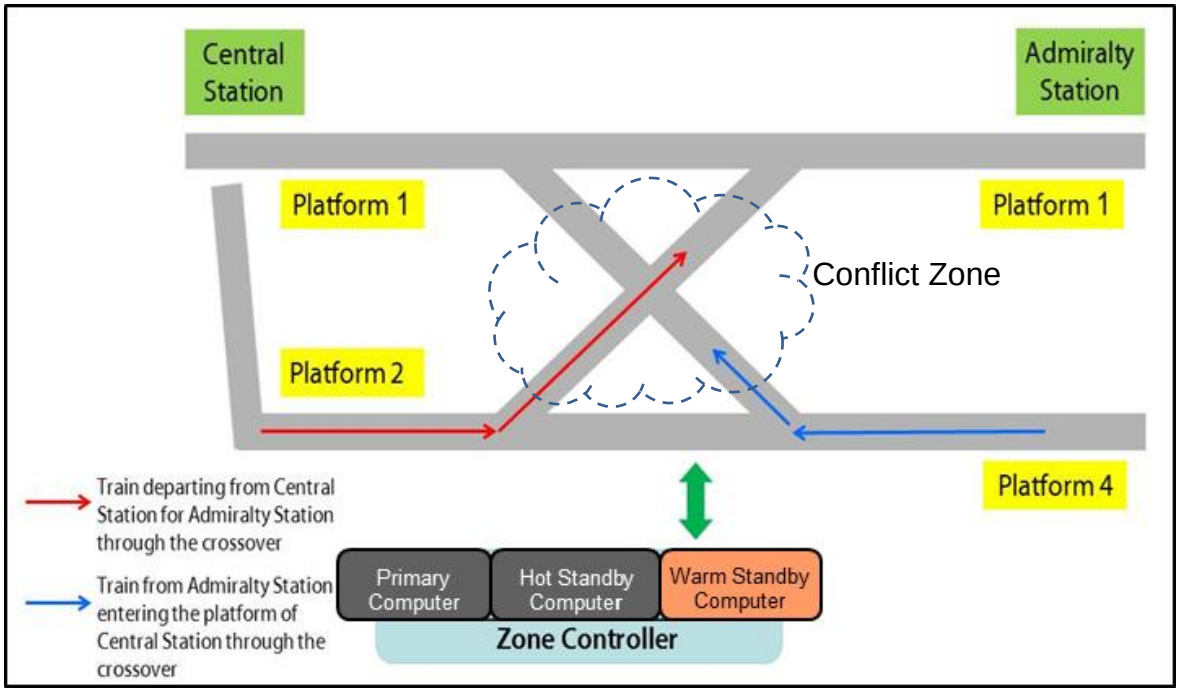
and trains were allowed to operate with minimum safe separating distance. Only for a specific test on Automatic Speed Control for stopping accuracy, was a separation of one station distance between trains required.

4. In January 2019, while there was no restriction on the number of trains, full line testing with 30 trains and with Computer C as Warm-standby was conducted. In other words, Computer C could have taken the overall operational control in case both Computers A and B had failed.

Annex 2

Incident of the New Signalling System Drill on Tsuen Wan Line on 18 March 2019

Illustration of the Scenario

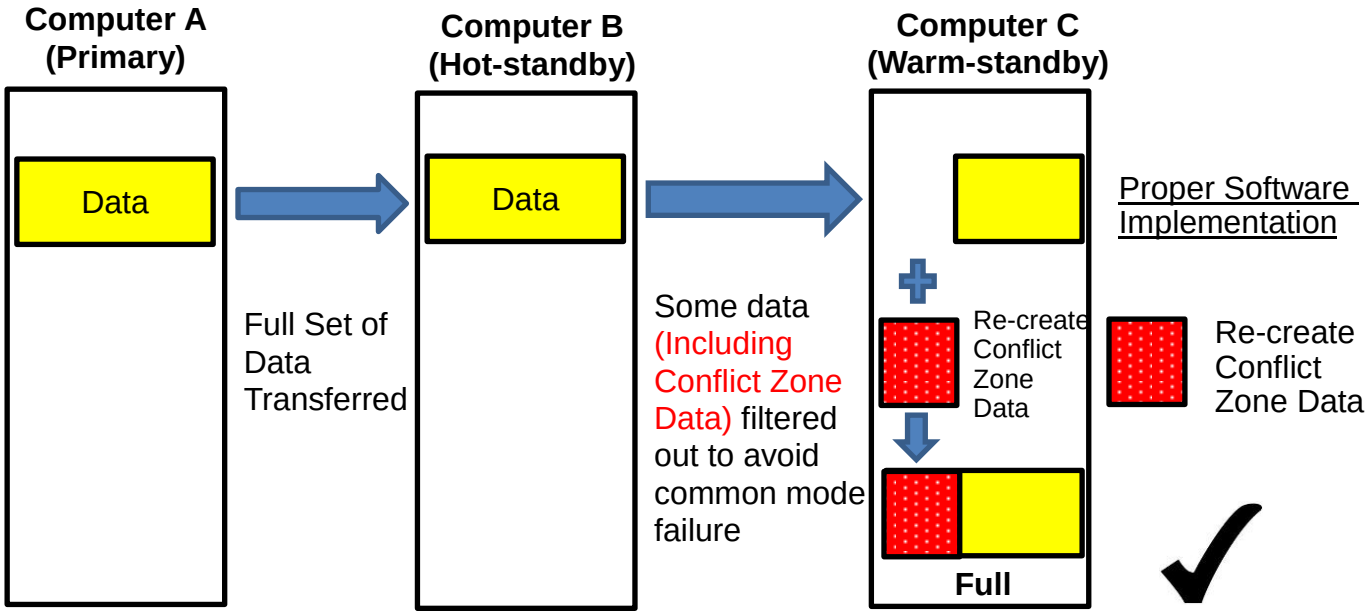


Annex 3

Data Transfer among the Three Computers A, B and C

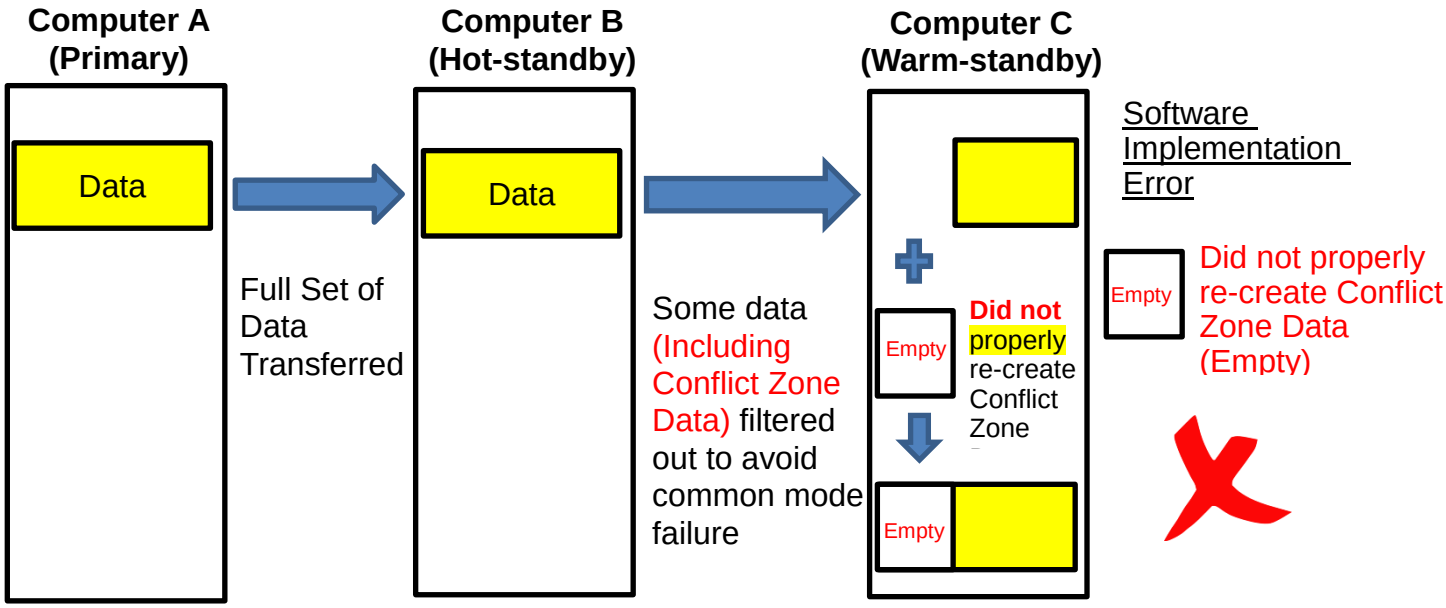
On 18 March, Computer A as "Primary" was switched off and made Computer B become "Primary", thereafter, Computer B was subsequently switched off and made Computer C become "Primary".

Design Intention developed by ATDJV



What Happened :

Software Implementation Errors resulted into an unknown software issue



Investigation Report on

Incident of the New Signalling System Testing on

MTR Tsuen Wan Line

港鐵荃灣綫

新信號系統測試事故

調查報告

Date of Incident: 18 March 2019

事故日期：2019 年 3 月 18 日

English Version

英文版

機電工程署 EMSD

Date of Issue: 5 July 2019

出版日期：2019 年 7 月 5 日

CONTENTS

	Page
Executive Summary	2
1. Objectives	4
2. Background of the Incident	4
3. Technical Information of the Incident Signalling System	7
4. Approach of Investigation	11
5. The EMSD Investigation Findings	12
6. Investigation Findings of Railway Experts Engaged by the EMSD	19
7. Conclusions	23
8. Measures Taken after the Incident	23
Appendix I – Drills and Exercises from 16 February to 18 March 2019	25
Appendix II – Sequence of Events	26
Appendix III – EMSD's views on the MTRCL Investigation Panel Report	27

Executive Summary

On 18 March 2019, a two-train collision incident happened during a drill and exercise on the new signalling system of the Tsuen Wan Line. This report presents the results of the Electrical and Mechanical Services Department's (EMSD) independent investigation into the causes of the incident.

The signalling system contractor Alstom-Thales DUAT Joint Venture (ATDJV), which is a joint venture of the Alstom Hong Kong Limited (Alstom) and the Thales Transport & Security (Hong Kong) (Thales), had been carrying out tests of the new signalling system in non-traffic hours at different sections of the Tsuen Wan Line by phases since late 2016. The tests carried out by the ATDJV for the entire section were completed in February 2019. On 16 February 2019, the MTR Corporation Limited (MTRCL) commenced the drills and exercises.

The incident occurred in non-traffic hours at 2:44 a.m. on 18 March 2019, when the MTRCL was conducting drills and exercises on the new signalling system of the Tsuen Wan Line. At the time of the incident, train T131, which was travelling from Admiralty Station to platform no. 1 of Central Station, collided with train T112, which was leaving Central Station for Admiralty Station, resulting in damage to the second to fourth cars of train T112 and derailment of two bogies of the first car of train T131. The train captains of both trains were taken to hospital for medical check and discharged on the same day.

According to our investigation findings, the cause of the incident was a programming error introduced during software rectification of the new signalling system at the design and development stage. This programming error caused a failure to re-create the data of the crossover track at Central Station after switch-over from the primary zone controller (ZC) to the warm-standby tertiary ZC. Hence, the Automatic Train Protection (ATP) system could not function as required to prevent two trains from entering the crossover track at Central Station at the same time, and led to the train collision.

The investigation also identified the following causes of the incident:

(a) the programming error, which was introduced in July 2017 during software rectification of the new signalling system, was not identified by the system contractor during various system testing / software upgrades as a result of

poorly specified design requirements and inadequate design, verification and validation processes of the software;

(b) the potential risk arising from the introduction of the warm-standby tertiary ZC was not comprehensively included in the risk assessment by the system contractor for the new signalling system; and

(c) simulation tests were not conducted to the maximum extent by the system contractor prior to the site tests, taking into account the specific requirement for a warm-standby tertiary ZC, which is a unique implementation by the supplier among the supplier's standard signalling system products.

Subsequent to the collision incident, the MTRCL had suspended all testing of the new signalling system on the Tsuen Wan Line, Island Line and Kwun Tong Line immediately. The MTRCL had also announced that all train tests for the new signalling system during non-traffic hours was suspended. The Government will allow the MTRCL to resume testing of the new signalling system of the Tsuen Wan Line only after the EMSD has ascertained the causes of the incident and remedial work has been completed satisfactorily.

The EMSD had also examined the MTRCL's Investigation Panel Report submitted on 17 June 2019 and the EMSD's views are listed at Appendix III.

Investigation Report on
Incident of the New Signalling System Testing on MTR Tsuen Wan Line
on 18 March 2019

1. Objectives

1.1 The purpose of this investigation is to identify the causes of a train collision during the new signalling system testing on the Tsuen Wan Line on 18 March 2019. This report presents the results of the EMSD independent investigation into the causes of the incident.

2. Background of the Incident

2.1 The signalling system contractor Alstom-Thales DUAT Joint Venture (ATDJV), which is a joint venture of the Alstom Hong Kong Limited (Alstom) and the Thales Transport & Security (Hong Kong) (Thales), had been carrying out tests of the new signalling system during non-traffic hours at different sections of the Tsuen Wan Line by phases since late 2016. The ATDJV commenced the full-line train tests in early 2018 and had substantially completed the tests on site, which lasted for more than two years, in February 2019. On 16 February 2019, the MTRCL commenced a series of drills and exercises (**Appendix I**) before putting the new signalling system into revenue service. From 16 February to 18 March 2019, the MTRCL conducted nine drills and exercises simulating various specific scenarios, including train fault, point failure as well as failure of both the primary and secondary zone controllers (ZC).

2.2 The incident occurred during non-traffic hours at 2:44 a.m. on 18 March 2019 (**Appendix II**), when the MTRCL was conducting the 9th drill and exercise on the new signalling system of the Tsuen Wan Line. Participating parties included the MTRCL's project staff, staff from its Operations Control Centre (OCC), station staff, train captains, and the ATDJV's engineering staff. The scenario of that particular drill and exercise was to simulate a failure of both the primary and secondary ZCs controlling the zone between Central Station and Sham Shui Po Station. The MTRCL arranged 34 trains to simulate train operation in a

situation where the warm-standby tertiary ZC[1]. would take over control from the faulty primary and secondary ZCs during peak hours, with a view to training up the MTRCL staff's response so as to maintain train operation in such situation.

2.3 According to the train logs, train T131, which was travelling from Admiralty Station to platform no. 1 of Central Station, collided with train T112 at a speed of 19 kph at the Central Station crossover track (Figure 1) at the time of the incident. At that moment, train T112 was travelling from Central Station to Admiralty Station at a speed of 31 kph when passing through the crossover track. The collision resulted in damages to the second to fourth cars of train T112 (Figure 2) and derailment of two bogies of the first car of train T131. The two train captains were taken to hospital for medical check and discharged on the same day.

Figure 1: Condition of the trains after collision

[1] Warm-standby is a redundancy system design. When the active primary ZC is in operation, the tertiary ZC remains in the warm-standby mode and obtains partial data from the primary ZC. Therefore, the data of the active primary ZC and the warm-standby tertiary ZC are not synchronised.

Figure 2: Damage to the saloon of train T112

2.4 According to the train logs and the train captains' interview records, the train captain of train T131 had pressed the emergency brake button before the collision to try to stop the train, but train T131 could not be stopped timely and collided with train T112. Moreover, according to the train logs, the ATP system could not function at that moment to restrict these two trains from entering into the crossover track at the same time. Figure 3 illustrates the train movements during the incident.

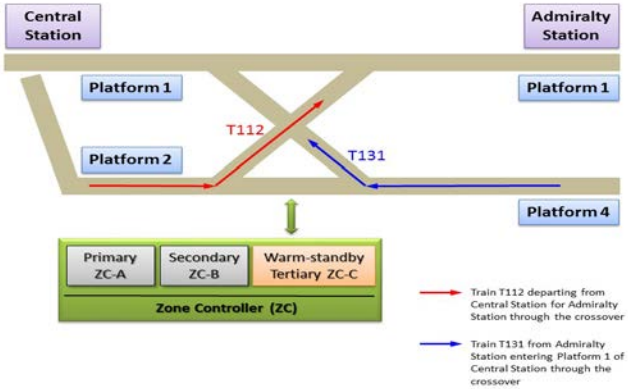


Figure 3: Train movements during the incident

2.5 The EMSD received notification of the incident at 3:03 a.m. and immediately dispatched staff to the scene for investigation.

2.6 During the drill and exercise on 18 March 2019, the existing signalling system was isolated. All trackside equipment and train-borne signalling equipment were under the control of the new signalling system. Unlike the existing signalling system and other signalling systems of the MTRCL's railway lines, this new signalling system was equipped with a unique tertiary ZC in warm-standby mode. Hence, this incident was not related to the existing signalling systems and similar incidents should not happen on existing railway lines.

3. Technical Information of the Incident Signalling System

3.1 In 2015, the MTRCL awarded a contract for upgrading the signalling systems of seven railway lines (Tsuen Wan Line, Island Line, Kwun Tong Line, Tseung Kwan O Line, Disneyland Resort Line, Tung Chung Line and Airport Express Line) to a joint venture company formed by two signalling system contractors, i.e. Alstom and Thales (known as the ATDJV). The target completion date is 2026.

3.2 A signalling system controls the safe operation of train services in railway network. Railway lines are divided into blocks and only one train is allowed in one block at any one time in order to ensure that trains are kept at a safe distance from each other. The present signalling system of the above-mentioned seven existing railway lines adopts a fixed block design[2], while the new signalling system adopts the "Communications Based Train Control" (CBTC) technology[3] using a moving block design to ensure that a safe distance between trains is still maintained even with increased train frequency and line capacity.

3.3 On 18 March 2019, the MTRCL conducted a drill and exercise on the new signalling system of the Tsuen Wan Line. Through wireless communication, trains sent information such as locations and speeds, etc. to the primary ZC, which

---

[2] With the fixed block concept, if a train is in a certain fixed block, the signalling system will send commands to the next train requesting it not to enter that block.

[3] The new signalling system uses wireless communication to transmit signals from trains (such as location and speed of trains) to the control computer. The computer then works out the safe distance required between trains.

calculated the safe distances between trains and sent limits of movement authority to the trains in order to achieve higher efficiency in train service management.

3.4 To further enhance the availability of the signalling system, the new signalling system of the Tsuen Wan Line has adopted a three-ZC configuration for train control, namely primary ZC A (ZC-A), secondary ZC B (ZC-B) and tertiary ZC C (ZC-C). This is a unique and non-standard design among its standard signalling system products of the supplier. The respective functions of the different ZCs are as follows (Figure 4):

(a) Primary ZC-A is the active ZC of the system for train control in the designated track section;

(b) Secondary ZC-B is the hot-standby ZC, which synchronises with ZC-A at all times and takes over ZC-A for train control as primary ZC when ZC-A fails;

(c) Tertiary ZC-C is the warm-standby ZC and takes over ZC-A and ZC-B as the active ZC when both ZC-A and ZC-B fail at the same time. To avoid common mode failure[4], part of ZC-C's data is not synchronised with ZC-A and ZC-B, which would be re-created in ZC-C upon taking over as the active ZC.

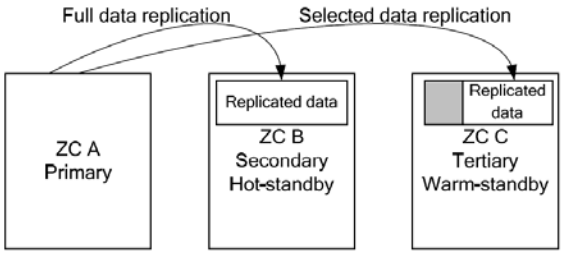


Figure 4: Design functions of the three ZCs

The addition of ZC-C in the new signalling system as warm-standby is a new design and its switch-over mode is more sophisticated than that of conventional design which adopts only two ZCs as active and hot-standby configurations.

[4] Common mode failure means that the same fault occurs at the tertiary warm-standby ZC when it takes over control as the active ZC from the primary ZC and the secondary hot-standby ZC.

3.5 Under all circumstances, only one ZC should be active in the signalling system to control the trains. The active ZC will receive information of operating trains and tracks at all times, including positions, speed, travelling direction and speed limit restriction of the trains at particular sections, points, and crossover positions. Not only does the active ZC calculate and maintain a safe distance between trains, it also restricts the simultaneous entry of more than one train into a point or crossover track to ensure safe railway operation.

3.6 Under normal conditions the active ZC will be either ZC-A or ZC-B. The active ZC regularly sends dynamic data to the warm-standby ZC-C every 100 milli-seconds. In order to minimise common mode failure, based on information extracted from the incident investigation report submitted by the supplier, the following six route-related data items would not be replicated from the active ZC (i.e. either ZC-A or ZC-B) to the warm-standby ZC (ZC-C) (Figure. 5) :

- Conflict zone
- Crawlback
- Crossline
- Border reservation
- Switch control
- Signal control

3.7 In the event when both ZC-A and ZC-B are faulty, the warm-standby ZC-C will act as the active ZC. In handling the route-related conflict zone data, the warm-standby ZC-C will first initialise its internal data space, then call a software subroutine to combine dynamic data collected from the corresponding trackside and signalling equipment with the corresponding static data (which is stored in the ZC-C database) for ZC-C to execute the signalling functions. These dynamic data include :

- Number of conflict zone objects
- Whether the conflict zone has overlapped with non-communicating objects
- Whether the conflict zone has overlapped with non-communicating objects during the previous cycle
- Number of users inside the conflict zone
- Train identification of the user
- Route identification of the user

The above dynamic data of the conflict zone, once collected from the trackside and signalling equipment, will be combined with the following two static data of the conflict zone in ZC-C:

- Conflict zone identification
- Number of paths set in the conflict zone

A complete and correct set of conflict zone data will be re-created based on the above dynamic data and static data for ZC-C to execute the signalling functions, including ATP to prevent train collision in the conflict zone.

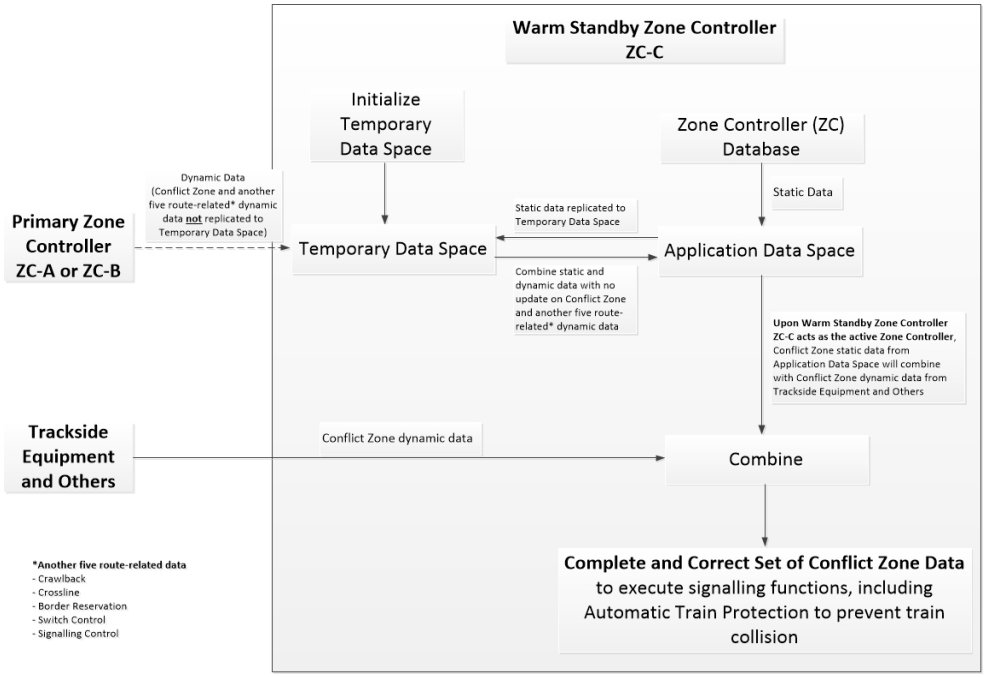


Figure 5: Integration of conflict zone data from primary/secondary ZCs, warm-standby tertiary ZC and trackside equipment

3.8 However, during the collision incident, due to programming error, the software subroutine mentioned above for conflict zone was not executed in the warm-standby ZC-C when it took up the active ZC role, and therefore the conflict zone data in ZC-C could not be re-created correctly. This error allowed two trains to enter the incident conflict zone and caused the collision.

4. Approach of Investigation

4.1 The EMSD conducted an independent, in-depth and comprehensive investigation into the causes of this incident. The EMSD also appointed three independent parties to provide expert advice, namely TPD System Asia Limited (TPDSA), an railway safety consultant with overseas experts in incident investigation, safety management and risk assessment of systems and processes; Professor Roderick Smith of the Imperial College, an expert in railway safety; and Professor Felix Schmid of the University of Birmingham, an expert in railway signalling systems. In carrying out the investigation, the EMSD has:

(a) conducted more than 65 meetings and reviewed over 250 documents and records, which cover 16 different document categories including project contract documents, design documents, testing and commissioning plans, testing and commissioning reports, testing certificates, procedures for drill and exercise, safety certificates, software programming codes, notes of meetings, recommendations from the Independent Safety Assessor (ISA) and the Independent Reviewer (IR) engaged by the MTRCL, traffic notices, safety briefing records, briefing records for drills and exercises, train logs and investigation reports;

(b) reviewed the traffic notices of the OCC, safety briefing records, briefing records for drill and exercise, incident train logs, trainborne signalling logs of the incident trains and ZC alarm logs on the day of the incident;

(c) reviewed the CCTV footage of the platform and concourse areas before and after the incident;

(d) reviewed the software programming versions of the incident ZCs and trainborne signalling equipment as well as conducted simulation tests on the three incident ZCs;

(e) reviewed the corresponding software programming codes;

(f) reviewed the investigation reports of the MTRCL and the ATDJV;

(g) interviewed 106 MTRCL staff, viz. 53 project team staff, 4 OCC staff, 11 station staff and 38 train captains;

(h) interviewed 27 project team staff from the ATDJV;

(i) interviewed 2 representatives from the ISA (Arthur D Little Limited); and

(j) interviewed 2 representatives from the IR (Kusieog Limited).

5. The EMSD Investigation Findings

5.1 Cause of Incident

According to the EMSD's investigation, the new signalling system performed differently from its intended operation as described in paragraph 3.7. On the day of the incident, the MTRCL performed a drill and exercise on site to simulate a failure in the primary and secondary ZCs, which controlled the stations between Central and Sham Shui Po during peak hours. The purpose of the drill and exercise was to train personnel from the MTRCL to cope with this failure. The scenario of the drill and exercise was that the primary ZC (ZC-A) and the secondary ZC (ZC-B) on hot-standby mode failed simultaneously, and that the signalling system had to be switched over to the tertiary ZC (ZC-C) on warm-standby mode to maintain train operation.

The investigation revealed, when ZC-C took up the active ZC role, the computer programme for handling conflict zone data did not execute the relevant subroutine to combine the dynamic data with the static data and did not re-create the conflict zone information correctly (Figure 6). Because the correct information on the conflict zone was not available, the conflict zone at the crossover track at Central Station did not exist in ZC-C. In the end, the ATP system could not function properly to prevent two trains from entering the crossover track simultaneously and resulted in the train collision.

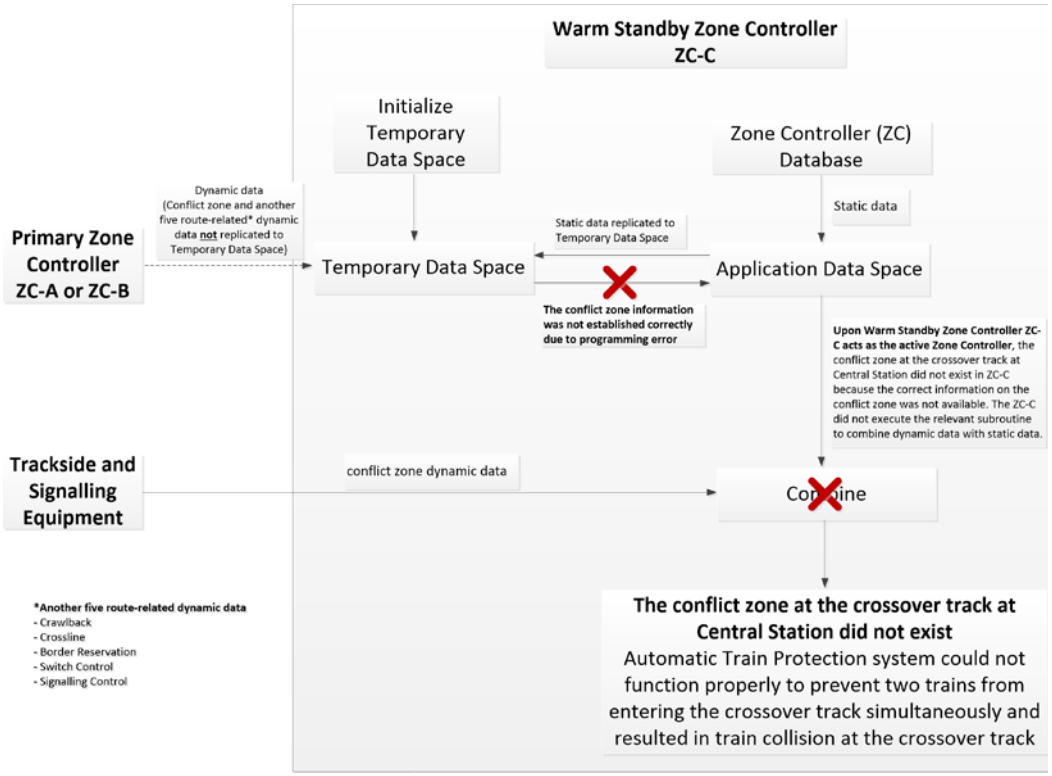


Figure 6: The tertiary ZC did not execute the relevant subroutine to combine the dynamic data with static data

5.1.1 Test items

After the incident, the EMSD and its appointed railway consultant performed multiple tests at the Kowloon Bay Depot, the Ho Man Tin Station[5], the ATDJV Office in Hong Kong and the ATDJV Software Development Centre in Toronto, Canada. The tests were as follows:

(a) Brake tests for the incident trains

A series of brake tests were performed on the incident train T131 at the Kowloon Bay Depot to test the operation of the brake system, with a view to ascertaining whether the incident was related to the brake system of the train. According to the test results, the brake system operated properly and hence was not related to the incident.

(b) Computer simulation tests for the signalling system

Computer simulation tests (Figures 7 and 8) were conducted at the Ho Man Tin Station, the ATDJV Office in Hong Kong and the ATDJV

[5] Ho Man Tin Station is equipped with a new signalling system simulator for training purpose.

Software Development Centre in Toronto by using the same software version as that of the trains in the incident, with the same location and conditions of the incident to ensure that the scenarios were identical. The test results of the simulations revealed that the same collision would happen by using the same software version in the simulators.

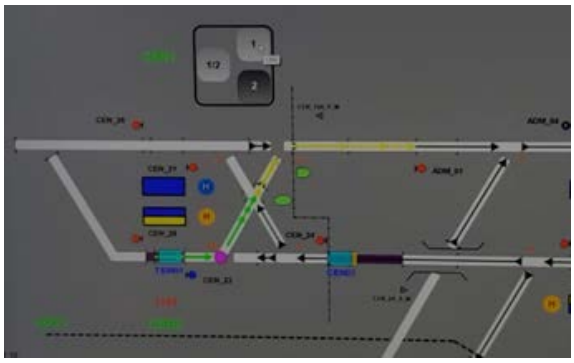


Figure 7: Simulator in ATDJV Hong Kong Office showed the route setting for trains T112 and T131 entering the conflict zone at Central Station at the same time.

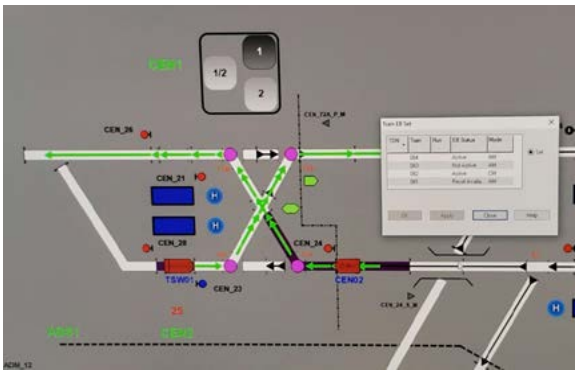


Figure 8: Simulator in ATDJV Hong Kong Office showed the trains entering the conflict zone at the same time at Central Station, as the route setting had allowed them to do so.

(c) Simulation tests for incident ZCs and vehicle on-board controllers (VOBCs)

Simulation tests (Figures 9 and 10) were conducted at Ho Man Tin Station by using the ZCs and VOBCs of the incident trains with the same location and conditions of the incident, with a view to ascertaining whether the incident was caused by the incident ZCs and VOBCs. According to the results of the simulations, the same incident would happen by using the incident ZCs and VOBCs in the simulator.

Figure 9: Simulator in Ho Man Tin Station

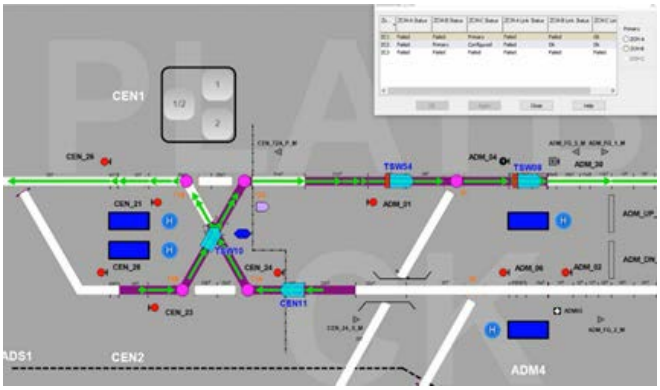


Figure 10: Simulation results showed the ZCs and VOBCs of the incident trains allowing the trains to enter the conflict zone at Central Station at the same time

5.2 Development, Verification and Testing of Signalling System and Drill and Exercise

5.2.1 Programming error in ZC

Investigation showed that there was a programming error in the signalling system software for ZCs after a modification of software coding in July 2017. Due to this programming error, when ZC-C was switched over to become the active ZC, the computer programme for handling conflict zone data did not execute the relevant subroutine to combine the dynamic data with static data, hence the conflict zone at Central Station could not be properly re-created in ZC-C. The ATP system could not function as required to prevent two trains from entering the crossover track at the Central Station at the same time and led to the train collision.

5.2.2 Development process of software programme

It is specified in BS EN 50128 (Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems) that the specification, functional requirements and programming logic of the software should be properly recorded during the development process to allow software developers to formulate relevant tests and reviews in the subsequent verification and validation process. The investigation revealed that the software coding of tertiary controller

ZC-C made in July 2017 regarding the conflict zone data had not been properly recorded in the software design, and therefore the related software coding error was not detected in the subsequent verification and validation process.

This means that the software design and the corresponding change request did not specify how to properly handle the re-creation of conflict zone data in ZC-C. The design and change control documents only mentioned that data related to existing route request, route authorisation and Limit of Movement Authority (LMA) would not be replicated to ZC-C, without mentioning that conflict zone data also would not be replicated to ZC-C. If the software developer had properly recorded all the specifications, functional requirements, programming logic and modifications made in the software, the error codes might have been identified and rectified in the subsequent verification and validation process.

5.2.3 Risk assessment for signalling system

A typical signalling system usually deploys two ZCs (i.e., primary ZC-A and secondary ZC-B) for switch-over between active and hot-standby modes. The provision of tertiary ZC in warm-standby mode in the new Tsuen Wan Line signalling system is a unique implementation by the supplier among the supplier's standard signalling system products. The investigation revealed that risk assessment had not been comprehensively conducted to address the potential hazards due to the unique design of ZC-C during system development. For the design of ZC-C in combining dynamic and static data of conflict zone, if the following activities, including detailed risk assessment, safety requirement identification, verification of safety documents in design documentation, implementation of safety requirements in design, review of design, implementation of the requirements in code, review of the code, and corresponding comprehensive simulation tests or on-site tests had been all properly conducted, the software coding errors might have been identified.

5.2.4 Verification and validation process

In view of the concerns and comments raised by the ISA engaged by the MTRCL, additional verification and validation checking on the software were conducted from October 2018 to February 2019. Most of the additional verification and validation checking were completed on 1 March

2019, but the above-mentioned software coding errors were not identified. The independent software assessment scheduled for February 2019 was not completed as scheduled. If such assessment had been completed in February 2019 as required, the software coding errors might have been identified. However, the EMSD's appointed consultant was of the view that the programming error might still not be identified in the above independent software assessment.

5.2.5 Testing of signalling system

The international standard, IEEE1474.4 (Recommended Practice for Functional Testing of a Communications-Based Train Control (CBTC) System), states that simulation tests to the maximum extent possible should be conducted during the stage of factory acceptance tests. Also that on-site functional tests should include functions of the whole signalling system (i.e. including ZC-C), so as to verify that the CBTC functional requirements are satisfied. According to records, comprehensive simulation tests of conflict route were not conducted for the incident scenario (i.e. both ZC-A and ZC-B failed, with ZC-C switched over to be the active ZC) during the factory functional testing stage and on-site functional testing stage. Had comprehensive simulation tests and on-site functional tests been conducted to the maximum extent possible, the programming error and the issue of the ZC-C being unable to re-create conflict zone data might have been identified.

5.2.6 Simulation of signalling system

The provision of tertiary ZC in warm-standby mode in the Tsuen Wan Line signalling system is a unique implementation by the supplier among the supplier's standard signalling system products. The specific requirements of tertiary ZC in warm-standby mode in signalling system were stipulated in the Particular Specification of the contract document. The design requirement was detailed in system design, which only stated the route request, route authorisation and LMA would not be replicated to ZC-C. If the design documents had covered details on the handling of conflict zone data upon ZC-C taking over as the active ZC, and more comprehensive simulation tests had been conducted for the non-standard design prior to the site tests, the corruption of the conflict zone data at the incident crossover track might have been discovered earlier and rectified and the incident on 18 March 2019 might not have happened.

5.2.7 Arrangement of on-site drills

The MTRCL engaged an ISA to certify the safety of the new signalling system before it is deployed to service. On the basis that the new signalling system was to be commissioned in mid-2019 as earlier planned. The ISA reported to the MTRCL on 19 October 2018 that the weaknesses of the signalling safety assurance system might result in an unsafe incident and improvements were required. The ISA raised the following comments on 6 February 2019 and reiterated the subject on 5 March 2019 that:

(a) they did not believe the signalling system fully complies with recognized international standards;

(b) they had significant concerns on compliance with the system developer's software development processes; and

(c) they did not believe that the development processes employed by the supplier are commensurate with the complexity of the signalling system. Many latent safety anomalies were identified on the system core software (Convergence 3.2) since the issue of the safety certification. These revealed the fundamental process weaknesses. The likelihood that such weaknesses might result in an unsafe incident was unacceptably high.

In response to the ISA's comments, the concerned parties carried out tri-partite workshops on 19-25 February 2019 to discuss the ISA's concerns and the system's development progress. After the meeting, the MTRCL postponed the planned service of the new signalling system by six months to Q4 of 2019 to allow time for the ATDJV to respond to the ISA's concerns and improve the new signalling system. The ATDJV indicated that a new version of the signalling system would be released on 24 May 2019. The new version is Build 8.3.4, whilst the version used in the incident was Build 8.3.3. According to records, both the ATDJV and the MTRCL, who participated in the drills and exercises, were aware of the scheduled release of the new software version in May 2019 and the content of the changes. While the said programming error that led to the incident were identified only after the incident, and was not included in the ATDJV's planned update items of the software in Build 8.3.4, we consider it there might still be a very remote chance that the ATDJV might have identified the programming error in the new build, or during software assessment or review to be conducted

by an independent software team of the ATDJV. Our appointed railway experts were of the view that there was no clear advice at the time that would have triggered the MTRCL to suspend the drills and exercises in the wait for the new software release, and that there was no evidence either the programming error would have been identified and rectified in the new version in any case.

5.2.8 Procedures of on-site drills

Drills and exercises commenced on 16 February 2019. The incident occurred during the 9th drill, in which 34 trains were deployed for on-site drills without making reference to any relevant drill procedures.

6. Investigation Findings of Railway Experts Engaged by the EMSD

6.1 Investigation Findings of Railway Consultant (TPDSA)

6.1.1 The EMSD has already established that the immediate cause of the collision was a software error in the tertiary Zone Controller (ZC-C) used to control the movement of trains prior to the engagement of TPDSA. TPDSA concurs that this is the immediate cause and has investigated the software defect in detail. TPDSA has also performed further investigations to establish why the error occurred and has identified the underlying causal factors as follows:

(a) A relatively brief examination of the software development processes showed significant deficiencies such that an undetected software error remained.

(b) The need of, or benefit from ZC-C has not been demonstrated and diluted the benefits of the proven core-software.

(c) There was no mapping of software requirements or independent review of the requirement interpretation at sub-system level.

(d) Until a late stage, the ISA had voiced out that the software development and safety engineering processes were inadequate and would affect the integrity of the finished product.

(e) The ISA scope was too limited. It did not cover "readiness for testing" either for one, or several trains, even though a Safety Case and Safety Certificate were produced by the supplier.

(f) The management of testing on the railway was poor with informal communication leading to assumptions and confusion as to the limits of testing and therefore insufficient controls applied.

(g) There was a lack of openness within the system contractor organisation and in its communication with the client. Communication broke down such that a PowerPoint presentation was wrongly interpreted as authority to proceed with any drills and exercises, even though the Safety Case and Safety Certificate had limitations.

(h) The Safety Case and Safety Certificate relating to the drills and exercises lacked clarity and traceability and there were gaps in the safety analysis arising from the introduction of the ZC-C such that compliance with EN50129 (Railway applications -Communication, signalling and processing systems - Safety related electronic systems for signalling) was not achieved.

(i) Programme and commercial pressures to start testing overtook the need for robust process to achieve correct software, the importance of which might not have been fully understood by the parties involved.

(j) The significance of latent safety defects identified in the core software and safety restrictions imposed on it were not understood as a precursor to poor process and therefore poor software. Decisions were made based on assumptions about the dependability of the core software that were shown to be unfounded.

(k) The operational staff (Traffic Controllers and Train Captains) could not reasonably have been expected to have done any more to prevent or mitigate the incident.

(l) The independent software assessment team is considered not sufficiently independent although they are from another unit of the supplier.

(m) The EMSD was kept at a distance in their regulatory role despite regular meetings. The difficult issues, such as the emerging ISA findings were not shared with the EMSD.

6.1.2 In summary, the requirement management, engineering safety management and software development processes were not in accordance with international standards EN50128 and EN50129, which were specified in the contract and are proven internationally for signalling systems. This led to an undetected error in their software.

6.1.3 A contributory cause was that warnings from the ISA that the software could not be relied on, were not fully resolved before the incident. In addition, the ISA remit did not cover "readiness for testing" even though a Safety Case and Safety Certificate were produced. The ISA's limited remit led to a situation where un-validated software without adequate safety controls was used for the drills and exercises for testing.

6.2 Investigation Findings of Professor Roderick Smith

6.2.1 The incident was caused by a weakness in the controlling software which failed to perform the necessary handshake of information when a test was performed to simulate the failure of the first two controllers. It is considered as a sound conclusion agreed by all related parties. This major conclusion is supported without reservation.

6.2.2 Doubts had been expressed by the ISA as early as October 2018 which were repeated in 6 February and 5 March 2019. These doubts contained comments such as lack of belief that the system fully complied with international standards and "latent anomalies" contained in the software might result in an unacceptably high risk of an unsafe incident. There followed tri-partite workshops between 19-25 February 2019 after which the introduction of the new system into revenue service was postponed to Q4 of 2019. This was the fourth of a series of push-backs from the original target of May 2018. This is very clear evidence that all parties were aware of difficulties arising from the testing prior to service introduction of this new system. A new version of the software was promised for May 2019. Between 16 February and the incident on 18 March eight further testing drills were conducted without any problems arising. At the time of the incident on 18 March, 34 trains were involved. There was no clear advice

issued by any party to the project proponent outlining the circumstances in further tests which would lead to unacceptable risk, nor any instruction to suspend testing until the new software became available.

6.2.3 Software has become increasingly complex and is being used in a huge variety of situations. It is difficult, perhaps impossible, to test complex software off-line for all eventualities. The authorship of such software is generally a team effort over a considerable period of time and many versions. Ensuring continuity is extremely difficult. The modelling of testing scenarios is only as good as the imaginations of the authors of the risk assessments prior to service introductions. There must be an element of reduction of probabilities in the testing and acceptance of software: a reduction of risk as far as reasonably practical is the goal and this will never be 100%. In this case new ground was being broken by the new signalling system.

6.3 Investigation Findings of Professor Felix Schmid

6.3.1 The significance of implementing a warm-standby rather than a hot- standby configuration in order to reduce the risk of a “data-driven” common-mode failure of all three ZCs, was not clearly understood by the stakeholders. In fact, the warm-standby system with three Zone Controllers A, B and C is a unique and non-standard design among its standard signalling system products of the supplier, which was requested specifically by the MTRCL to satisfy their exacting availability targets.

6.3.2 Individually, both the implementation of a CBTC system on an existing operating railway, and the introduction of a tertiary ZC-C would be deemed major changes. The criticality of combining the two changes was not recognized by the stakeholders.

6.3.3 The non-replication of conflict zone data to tertiary ZC-C should have been detailed in the system design document and in the subsequent formulation of simulation and field testing.

6.3.4 The non-replication of conflict zone data to tertiary ZC-C is not detailed in the system design document. Hence in addition to the programming (logic) omission, the poor system design documentation, the inadequate formulation of simulation and field testing were contributing factors.

7. Conclusions

Based on the investigation findings of the causes of the incident, the EMSD concludes that the train collision incident at the crossover track at the Central Station on Tsuen Wan Line during the drill and exercise in non-traffic hours on 18 March 2019 was due to the following reasons:

(a) there was a programming error in the software of the warm-standby tertiary ZC involved in the incident, resulting in a failure to re-create conflict zone data of the crossover track at the Central Station after switch-over from the primary ZC to the warm-standby tertiary ZC. Hence, the ATP system could not function as required to prevent two trains from entering the crossover track at the Central Station at the same time and led to the train collision;

(b) the programming error, which was introduced in July 2017 during software rectification of the new signalling system, was not identified by the system contractor during various system testing / software upgrades as a result of poorly specified design requirements and inadequate verification and validation processes of the software;

(c) the potential risk arising from the introduction of the warm-standby tertiary ZC was not comprehensively included in the risk assessment by the system contractor for the new signalling system; and

(d) simulation tests were not conducted to the maximum extent by the system contractor prior to the site tests, taking into account the specific requirement for a warm-standby tertiary ZC, which is a unique implementation by the supplier among the supplier's standard signalling system products.

8. Measures Taken after the Incident

8.1 Subsequent to the collision incident, the MTRCL has suspended all testing of the new signalling system on the Tsuen Wan Line, Island Line and Kwun Tong Line immediately. The MTRCL has also announced that all train tests for the new signalling system during non-traffic hours would continue to be suspended until the root cause of the incident has been identified.

8.2 The EMSD notes that the MTRCL Investigation Panel has made a number of recommendations to the system contractor and the MTRCL, and agrees that such recommendations aim to rectify the programming error and enhance the development and testing process of the new signalling system, with a view to preventing recurrence of similar incident. The EMSD will monitor the MTRCL's full implementation of the measures and assess the effectiveness of such. The Government will only allow the MTRCL to resume train testing of the new signalling system after the MTRCL has fully completed the remedial work and the EMSD has confirmed the safety of the new signalling system upon inspection.

- End of Report -

Appendix I – Drills and Exercises from 16 February to 18 March 2019

Date	Drills and Exercises
16 Feb 2019	Drills and Exercises No. 1 Simulate points machine failure and train fault
21 Feb 2019	Drills and Exercises No. 2 Simulate OCC blackout, OCC evacuation and other operational exercise
23 Feb 2019	Drills and Exercises No. 3 Simulate Smart I/O failure and assisting train
28 Feb 2019	Drills and Exercises No. 4 Simulate power supply failure and docking failure
9 Mar 2019	Drills and Exercises No. 5 Simulate power supply failure and docking failure
12 Mar 2019	Drills and Exercises No. 6 Simulate Smart I/O failure
15 Mar 2019	Drills and Exercises No. 7 Simulate OCC blackout, OCC evacuation and other operational exercise
17 Mar 2019	Drills and Exercises No. 8 Simulate assisting train
18 Mar 2019 (Date of incident)	Drills and Exercises No. 9 Simulate ZC failure

Appendix II – Sequence of Events

Time	Description
18 March	
0:15 a.m.	The ATDJV conducted briefing to the MTRCL staff, followed by briefing to the MTRCL staff by the MTRCL's drills and exercises in-charge.
2:44 a.m.	Two trains collided at Central Station.
2:54 a.m.	The Fire Services Department and Hong Kong Police Force were notified of the incident. The two train captains were sent to the hospital for medical check, and were discharged on the same day.
2:56 a.m.	The Transport Department (TD) was informed of the incident.
3:03 a.m.	The EMSD was informed of the incident.
3:17 a.m.	The TD was informed regarding the service disruption of Tsuen Wan Line.
4:00 a.m.	"Red alert" issued by the MTRCL. Passengers were informed of the Tsuen Wan Line service disruption through Traffic News and the media. Train service between Admiralty Station and Central Station of Tsuen Wan Line was temporarily suspended.
19 March	
Full Day	Recovery works in progress.
11:00 p.m.	Two bogies of one of the trains were re-railed.
20 March	
0:00 a.m. to 1:15 a.m.	Recovery works in progress.
1:15 a.m.	The trains were moved to the sidings of Admiralty Station and safety inspection was conducted after completion of the recovery works.

Appendix III – EMSD's views on the MTRCL Investigation Panel Report

There is no conflict on the investigation findings between the EMSD Investigation Report and the MTRCL Investigation Panel Report. Nevertheless, the EMSD considers the other facts and factors below are relevant to the incident:

(a) The provision of tertiary ZC in warm-standby mode is a unique and non-standard design among its standard signalling system products of the supplier, as such comprehensive risk assessments should be taken by the supplier and should not be limited by the software development document; and

(b) The simulation tests for the tertiary ZC during the stage of the factory acceptance tests could have been conducted comprehensively by the supplier because of its unique and non-standard design. The scope of simulation tests for tertiary ZC should make reference to IEEE1474.4 be of maximum extent and should not be limited by the software development document.

Besides, the MTRCL's Investigation Panel Report mainly focused on the deficiencies of the supplier in software development and system implementation processes. The Report did not mention the roles of the MTRCL Operations Project Team in overseeing the project implementation. The EMSD considers that, having regard to the significance of this project and the fact that the system design being a non-standard one, the MTRCL should avoid over-reliance on the contractor but ought to be extra vigilant at all times.

The EMSD also notes in the MTRCL's Investigation Panel Report that the Panel has recommended the ATDJV and the MTR Operations Project Team to implement a number of improvement measures to rectify the programming error and enhance the development process of the new signalling system (including the testing), with a view to preventing recurrence of similar incident. Specifically, the MTRCL has undertaken to –

(a) expand the scope of the ISA from safety assurance for passenger service to the inclusion of on-site train-related testing certification;

(b) upgrade the Training Simulator in Hong Kong to act as a testing simulation tool to perform more scenario simulation tests as far as practicable;

(c) establish a joint safety Test & Commissioning Panel (MTRCL/ATDJV together with input from the ISA) to manage on-site testing; and

(d) explore together with the Panel's experts on the merits, if any, for staging the development of the warm-standby computer, or any other technically appropriate alternatives proposed by the ATDJV.

The EMSD will monitor the MTRCL's full implementation of the measures and assess the effectiveness of such. The Government will only allow the MTRCL to resume train testing of the new signalling system after the MTRCL has fully completed the remedial work and the EMSD has confirmed the safety of the new signalling system upon inspection.